

ARITHMETIC OF DOUBLE TORUS QUOTIENTS AND THE DISTRIBUTION OF PERIODIC TORUS ORBITS

ILYA KHAYUTIN

ABSTRACT. We describe new arithmetic invariants for pairs of torus orbits on inner forms of \mathbf{PGL}_n and \mathbf{SL}_n over number fields. These invariants are constructed by studying the double quotient of a linear algebraic group by a maximal torus.

Using the new invariants we significantly strengthen results towards the equidistribution of packets of periodic torus orbits on higher rank S -arithmetic quotients. Packets of periodic torus orbits are natural collections of torus orbits coming from a single adelic torus and are closely related to class groups of number fields. The distribution of these orbits is akin to the distribution of integral points on homogeneous algebraic varieties with a torus stabilizer.

The proof combines geometric invariant theory, Galois actions, local arithmetic estimates and homogeneous dynamics.

CONTENTS

1. Introduction	1
2. The General Setting and Homogeneous Toral Sets	14
3. Geometric Invariant Theory of a Double Quotient by a Torus	16
4. Double Torus Quotient for \mathbf{SL}_n and \mathbf{PGL}_n	19
5. Double Torus Quotient for \mathbf{PGL}_2	26
6. Double Torus Quotient for Central Simple Algebras	29
7. Packets in Central Simple Algebras	36
8. Lower Bound for Asymptotic Entropy	48
9. Rigidity of Limit Measures	56
References	59

1. INTRODUCTION

1.1. Background. Let \mathbf{G} be a reductive linear algebraic group and $\mathbf{H} < \mathbf{G}$ a maximal torus, both defined over a number field \mathbb{F} . Many interesting affine algebraic varieties arise in the form $\mathbf{V} := \mathbf{G}/\mathbf{H}$. Our main interest is the way that families of integral points of \mathbf{V} , defined in a suitable sense, distribute in $\mathbf{V}(\mathbb{R})$ or in related S -arithmetic spaces.

We begin by examining several special cases. For simplicity of the exposition we assume $\mathbb{F} = \mathbb{Q}$.

1.2. Periodic torus orbits on $\mathbf{PGL}_n(\mathbb{Z}) \backslash \mathbf{PGL}_n(\mathbb{R})$. Consider the case that $\mathbf{G} = \mathbf{PGL}_n$ and \mathbf{H} is the maximal torus equal to the projection of the diagonal subgroup in \mathbf{GL}_n to \mathbf{PGL}_n . We wish to state a special case of our theorem adapted to this setting.

Following [ELMV09] we say that an $H := \mathbf{H}(\mathbb{R})$ orbit on

$$X := \mathbf{PGL}_n(\mathbb{Z}) \backslash \mathbf{PGL}_n(\mathbb{R})$$

is periodic if it supports an H invariant probability measure.

The periodic H orbits on X are grouped into natural finite collections called *packets*. To each packet of H -orbits corresponds, in a non-unique way, a totally real degree n field extension of \mathbb{Q} . The periodic orbits in the simplest packets are a principal homogeneous space for the class group of the associated number field¹, see [ELMV09, Corollary 4.4]. Notice, that these H orbits tautologically correspond to some $\mathbf{PGL}_n(\mathbb{Z})$ orbits on $\mathbf{PGL}_n(\mathbb{R}) / \mathbf{H}(\mathbb{R})$. Periodic H orbits on $\mathbf{PGL}_n(\mathbb{Z}) \backslash \mathbf{PGL}_n(\mathbb{R})$ necessarily correspond to orbits of $\mathbf{PGL}_n(\mathbb{Z})$ on *rational points* of $\mathbf{PGL}_n(\mathbb{R}) / \mathbf{H}(\mathbb{R})$.

To each packet one can associate the *discriminant*. This is an arithmetic property of the packet, in the case described above it is just the discriminant of the associated number field.

For $n = 2$ the space $\mathbf{PGL}_2(\mathbb{Z}) \backslash \mathbf{PGL}_2(\mathbb{R})$ is the unit tangent bundle of the modular surface. On this space periodic H orbits are exactly the non-divergent closed geodesics. There is a natural bijection on the modular surface between non-divergent closed geodesics and ideal classes in Picard groups of quadratic totally real orders, see [ELMV12]. In this case, the packets are exactly the collections of closed geodesics corresponding to the Picard group of a single order.

In general, each such packet supports a unique H invariant probability measure. Suppose we are given a sequence of packets $\{Z_i\}_{i=1}^{\infty}$ with discriminants D_i and H invariant measures μ_i . How the measures μ_i distribute on X when $D_i \rightarrow_{i \rightarrow \infty} \infty$?

When $n = 2$ these measure converge to the Haar measure. This has been proved by Duke [Duk88] building on a breakthrough of Iwaniec [Iwa87]. Duke's proof is based on harmonic analysis. For $n = 3$ see the recent results of [ELMV11] which we briefly review in §1.9. For higher n our state of knowledge is not as satisfactory. Assuming non-escape of mass, only a lower bound on the metric entropy of a limit measure is known [ELMV09, Theorem 3.1], see also Remark 1.3. We present a significant improvement for this lower bound for packets satisfying a Galois condition.

For any $a \in H$ and ν a probability measure on X invariant under H , denote by $h_\nu(a)$ the metric entropy of ν with respect to the action by a . Let

¹In general one needs to consider Picard groups of non-maximal orders in these number fields.

$h_{\text{Haar}}(a)$ be the entropy of the Haar probability measure on X , which is the unique measure of maximal entropy. In this setting we have the following special case of our main theorem.

Theorem 1.1. *Set $H < \mathbf{PGL}_n(\mathbb{R})$ to be a fixed maximal torus such that $\text{rank}_{\mathbb{R}} H > 0$, i.e. H is isotropic over the reals but not necessarily split.*

Let $\{Z_i\}_{i=1}^{\infty}$ be a sequence of packets of periodic H -orbits with discriminants D_i associated to maximal orders in number fields. Assume $D_i \rightarrow_{i \rightarrow \infty} \infty$.

Let \mathbb{K}_i be the totally real degree n field extension of \mathbb{Q} associated to Z_i . Denote by \mathbb{L}_i the Galois closure of \mathbb{K}_i . Assume for all i that $\text{Gal}(\mathbb{L}_i/\mathbb{Q})$ is 2-transitive when considered as a subgroup of S_n .

Let μ_i be the unique H invariant probability measure supported on Z_i . If μ_i converges in the weak- topology to a probability measure μ on X then for any $a \in H$*

$$h_{\mu}(a) \geq \frac{h_{\text{Haar}}(a)}{2(n-1)}$$

This theorem should be compared with [ELMV09, Theorem 3.1] which for H – the *totally split torus* of diagonal matrices and

$$a = \text{diag} \left(\exp \left(\frac{n-1}{2} \right), \exp \left(\frac{n-3}{2} \right), \dots, \exp \left(-\frac{n-1}{2} \right) \right)$$

provides the bound $h_{\mu}(a) \geq \frac{3h_{\text{Haar}}(a)}{(n+1)n(n-1)}$ without assuming a Galois condition and without a restriction to maximal orders.

The strength of our result compared to [ELMV09, Theorem 3.1] is that it is valid even when H is not totally split over \mathbb{R} and the significantly improved bound on the entropy under a Galois condition, especially for large values of n .

The entropy of the measure μ with respect to the action by a semisimple element $a \in \mathbf{PGL}_n(\mathbb{R})$ is related to the dimension of μ along its sections in some directions transversal to the direction of the a -action; specifically, directions in the unstable foliation. When the centralizer of a is not minimal the measure might have non-trivial sections in many transversal direction which do not affect the entropy. This is a significant problem when trying to bound the entropy with respect to an action by an element which has a big centralizer, as is the case for non totally split tori in our setting. The action of the Galois group of the splitting field on appropriate invariants we construct is an important ingredient in overcoming this problem. The method of proof of [ELMV09, Theorem 3.1] is fundamentally limited for a whose centralizer is minimal, hence the restriction to totally split tori in that result.

To prove this theorem we construct new invariants by analyzing the double quotient of \mathbf{G} by a maximal torus. A main tool for this is geometric invariant theory. Another novel aspect of our method is that we are able to utilize properties of the Galois groups of splitting fields.

In §1.5 we discuss the general notions of homogeneous toral sets and packets, followed by a statement of a complete version of our main theorem.

Beforehand we review one more classical example which serves as a motivation and where the role of integral points is apparent.

1.3. Points on Sphere. The 2-dimensional sphere \mathbf{S}^2 is the affine variety over $\mathbb{F} = \mathbb{Q}$ defined by the equation

$$x_1^2 + x_2^2 + x_3^2 = 1$$

This variety is equipped with a transitive action of $\mathbf{G} = \mathbf{SO}_3$. The stabilizer of a point is a conjugate of $\mathbf{H} = \mathbf{SO}_2 < \mathbf{SO}_3$. Thus we can identify $\mathbf{S}^2 \cong \mathbf{SO}_3/\mathbf{SO}_2 = \mathbf{G}/\mathbf{H}$. Indeed, $\mathbf{H} = \mathbf{SO}_2$ is a maximal torus of absolute rank 1 in \mathbf{G} .

Let $d \in \mathbb{N}$, consider the *integral* solutions to the equation

$$(1) \quad x_1^2 + x_2^2 + x_3^2 = d$$

Denote by \mathcal{H}_d the set of *primitive* integral solutions to (1). By Legendre's three square theorem $\mathcal{H}_d \neq \emptyset$ if $d \neq 4^a(8b+7)$ for all $a, b \in \mathbb{N}$. Accordingly, when writing $d \rightarrow \infty$ we consider only those d for which there are integral solutions to (1).

If integral solutions exist we denote by $\widetilde{\mathcal{H}}_d := \{x/\sqrt{d} \mid x \in \mathcal{H}_d\}$ the radial projection of \mathcal{H}_d to the unit sphere $\mathbf{S}^2(\mathbb{R})$. Let m be the unique $\mathbf{SO}_n(\mathbb{R})$ invariant probability measure on the sphere. We say that the collections \mathcal{H}_d equidistribute as $d \rightarrow \infty$ if for any continuous $f \in C(\mathbf{S}^2(\mathbb{R}))$

$$\frac{1}{|\mathcal{H}_d|} \sum_{x \in \mathcal{H}_d} f(x) \xrightarrow{d \rightarrow \infty} \int f(x) dm(x)$$

This is weak-* convergence of measures. The question whether equidistribution holds when the limit is taken along all possible d 's or along specific subsequences of d 's is well studied both using analytic number theory and homogeneous dynamics. This problem is closely related to the one we described in §1.2. Indeed the sphere is a homogeneous space for the projective group of units of the Hamilton quaternion algebra, which is an inner form of \mathbf{PGL}_2 . The equidistribution of $\widetilde{\mathcal{H}}_d$ on the sphere has been also settled by Duke [Duk88] using harmonic analysis.

Much before the appearance of the harmonic analytic solution, Linnik developed in the first half to the 20'th century his "ergodic method"; using which he was able to prove in the 1950's the equidistribution of integral points for specific sequences of d 's [Lin57], [Lin60]. Specifically, he needed the sequence $(d_i)_{i=1}^\infty$ to satisfy a splitting condition; he assumed that there is a fixed odd prime p such that p splits in all the field extension $\mathbb{Q}(\sqrt{-d_i})$. Under the hood of Linnik's original proof is the action of the split torus $\mathbf{SO}_2(\mathbb{Q}_p)$. This is the reason why the splitting condition for p appears.

Equidistribution of the points $\widetilde{\mathcal{H}}_d$ is equivalent to the equidistribution of packets of periodic $\mathbf{SO}_2(\mathbb{Q}_p)$ orbits on the S -arithmetic quotient

$$\Gamma \backslash G_S = \mathbf{SO}_3(\mathbb{Z}[1/p]) \backslash \mathbf{SO}_3(\mathbb{R}) \times \mathbf{SO}_3(\mathbb{Q}_p)$$

1.4. The Modern Variant of Linnik's Method. In a series of papers [ELMV09], [ELMV11], [ELMV12], Einsiedler, Lindenstrauss, Michel and Venkatesh have put forward a modern variant of Linnik's method.

In the modern viewpoint, Linnik's method is based upon the dynamics of a torus, e.g. $\mathbf{SO}_2(\mathbb{Q}_p)$, on an S -arithmetic space. In particular, this approach has analogues which use a fixed split archimedean torus. This can be used, for example, to prove Duke's result about the equidistribution of packets of closed geodesics on the modular surface [ELMV12]².

It is essentially a result of Gauss that there is an action of the Picard group of a quadratic order on \mathcal{H}_d . When d is square free this order is $\mathbb{Z}[\sqrt{-d}]$. This allows to compute the total volume of the periodic orbits corresponding to \mathcal{H}_d in terms of the class number of an order in the field $\mathbb{Q}(\sqrt{-d})$. As a result, Dirichlet's class number formula and Siegel's lower bound on the residue at 1 of a Dedekind ζ -function imply that this volume is $d^{1/2+o_d(1)}$.

The gist of the method is first to use an arithmetic well-separateness result for the orbits together with the volume computation above to derive an estimate for the metric entropy of any limit measure with respect to an element of the acting torus, e.g. $\mathbf{SO}_2(\mathbb{Q}_p)$. This entropy estimate is the input to a measure rigidity theorem which supplies the final result about the limiting distribution.

This general proof scheme has been exploited by Einsiedler, Lindenstrauss, Michel and Venkatesh in [ELMV09] and [ELMV11] to obtain fundamentally new results in higher rank analogues which we discuss in the next section.

The measure rigidity theorem used in the modern variant of Linnik's rank 1 argument in [ELMV12] is the uniqueness of measure of maximal entropy for the action of a semisimple element in the group. In higher rank significantly finer measure rigidity theorems are necessary to obtain results regarding the distribution of packets. These measure rigidity results are available due to the works of Lindenstrauss [Lin06]; Katok, Einsiedler and Lindenstrauss [EKL06] and [EL15].

The arithmetic well-separateness part in Linnik's original argument for the 2-sphere is Linnik's basic lemma. Its proof depends on counting representations of a binary integral quadratic form by a ternary one. This

²This has been achieved in the framework of Linnik's original method by Skubenko [Sku62] using again what amounts to the action over a fixed finite prime p . In particular, Skubenko's argument required a splitting condition at p while the argument of [ELMV12] does not because it is able to use the split real torus.

counting argument is converted to a result about average separation between orbits using a basic invariant - the euclidean inner product of two integral points on the sphere.

The main contribution of the work presented here is a generalization of this invariant to higher rank and the analysis of some fundamental properties of the new invariants. It is using these results that we are able to prove an improved bound on the limit entropy in higher rank spaces.

1.5. Higher Rank Spaces. In the example of the 2-sphere \mathbf{G} had absolute rank 1, accordingly the torus \mathbf{H} has been a rank 1 torus. We return to higher rank cases.

Although some of our results apply to any reductive group \mathbf{G} , our major focus is on groups of units in central simple algebras, i.e. inner forms of \mathbf{PGL}_n and \mathbf{SL}_n .

Systematic higher rank results directly in the spirit of Linnik's and Duke's rank 1 theorems have been achieved in [ELMV09] and in [ELMV11]. Related problems have been studied extensively already by Eskin, Mozes and Shah [EMS96] and Benoist and Oh [BO07].

We discuss briefly the more general case when \mathbf{G} is a linear algebraic group and \mathbf{H} is a maximal torus, defined over a number field \mathbb{F} . We now fix a set of places S of \mathbb{F} including all the archimedean ones. Let $G_S := \prod_{u \in S} \mathbf{G}(\mathbb{F}_u)$ and let $\Gamma < G_S$ be a congruence lattice.

Fix a place $\hat{u} \in S$ and denote $\hat{\mathbb{F}} = \mathbb{F}_{\hat{u}}$, our object of study is orbits of the group $H := \mathbf{H}(\hat{\mathbb{F}})$ on the locally homogeneous space $\Gamma \backslash G_S$.

1.5.1. Packets of Periodic Torus Orbits. On $\mathbf{PGL}_n(\mathbb{Z}) \backslash \mathbf{PGL}_n(\mathbb{R})$ we had discussed packets of periodic torus orbits associated to class groups of totally real number fields. On the sphere we had discussed packets of periodic torus orbits associated to the collection \mathcal{H}_d of primitive integral solutions to (1). What would be a natural generalization of such collections to the general setting?

First we take a slightly different view point on periodic orbits. Let $g_S = (g_u)_{u \in S} \in G_S$, the H orbit $\Gamma g_S H$ can be written as $\Gamma(g_S H g_S^{-1})g_S$. If we define the algebraic torus³ $\mathbf{T} = g_{\hat{u}} \mathbf{H} g_{\hat{u}}^{-1}$ then we can write

$$\Gamma g H = \Gamma \mathbf{T}(\hat{\mathbb{F}}) g_S$$

The torus \mathbf{T} is a priori defined only over $\hat{\mathbb{F}}$. It turns out that the orbit $\Gamma g H$ is periodic, viz. supports an H invariant probability measure, if and only if the torus \mathbf{T} is defined and anisotropic over \mathbb{F} ; see [Oh04] and [ELMV09] for details.

Einsiedler, Lindenstrauss, Michel and Venkatesh suggest in [ELMV11, §4.1] an adelic approach to define *packets*, which are collections of periodic H orbits, for any linear reductive group \mathbf{G} .

³Notice that we conjugate only by the \hat{u} part of g_S .

Let \mathbb{A} be the adèle ring of \mathbb{F} . Under mild assumptions, the space $\Gamma \backslash G_S$ can be identified with a quotient of the adelic locally homogeneous space $\mathbf{G}(\mathbb{F}) \backslash \mathbf{G}(\mathbb{A})$, see §2.2.

For *any* maximal torus \mathbf{T} defined and anisotropic over \mathbb{F} and any $g_{\mathbb{A}} \in \mathbf{G}(\mathbb{A})$ one can define the associated homogeneous toral set to be

$$Y = \mathbf{G}(\mathbb{F}) \backslash \mathbf{T}(\mathbb{A}) g_{\mathbb{A}}$$

Notice that the definition of a general homogeneous toral set does not even require a fixed torus \mathbf{H} . If $g_{\mathbb{A}} = g_S$ and $\mathbf{T} = g_{\hat{u}} \mathbf{H} g_{\hat{u}}^{-1}$ then the projection of Y to the S -arithmetic quotient $\Gamma \backslash G_S$ will include the orbit $\Gamma g H$; but it might include many other periodic H orbits as well. A packet is the projection to the S -arithmetic space of a single homogeneous toral set in the adelic space.

The notion of a packet is an apt generalization of the collection \mathcal{H}_d in many aspects. Each homogeneous toral set and its associated packet have two basic properties. The first one is the volume of the homogeneous toral set, $\text{vol}(Y)$. The volume generalizes the size of the set \mathcal{H}_d . The second property is an arithmetic quantity called the global discriminant. The global discriminant generalizes the discriminant of the order in $\mathbb{Q}(\sqrt{-d})$ whose Picard group acts on \mathcal{H}_d . The global discriminant is a product of local discriminants for each place of \mathbb{F} , the local discriminant generalizes the absolute local discriminant of the order in $\mathbb{Q}(\sqrt{-d})$. We present these definition in §2.4.

For $\mathbf{G} = \mathbf{PGL}_n$ the volume $\text{vol}(Y)$ and the discriminant D are related to each other much in the same way as for \mathcal{H}_d

$$\text{vol}(Y) = D^{1/2+o(1)}$$

see [ELMV11, Theorem 4.8].

1.6. Main Theorem: Lower Bound on Asymptotic Entropy. Let \mathbf{B} be a central simple algebra over a number field \mathbb{F} . Let $\Omega \subseteq \mathbf{B}(\mathbb{F})$ be an $\mathcal{O}_{\mathbb{F}}$ order.

Let S be a finite set of places of \mathbb{F} including all the archimedean ones. Denote $\mathbb{F}_S = \prod_{u \in S} \mathbb{F}_u$. Suppose S includes at least one place over which \mathbf{B} is isotropic and that it is large enough so that $\mathbf{PGL}_1(\mathbf{B})(\mathbb{A})$ and $\mathbf{SL}_1(\mathbf{B})(\mathbb{A})$ have class number one with respect to the integral structure induced by Ω . If we denote by Ω_u the closure of Ω in $\mathbf{B}(\mathbb{F}_u)$ for each nonarchimedean place u , then the class number 1 requirement amounts to

$$\mathbf{PGL}_1(\mathbf{B})(\mathbb{A}) = \mathbf{PGL}_1(\mathbf{B})(\mathbb{F}) \cdot \mathbf{PGL}_1(\mathbf{B})(\mathbb{F}_S) \cdot \prod_{u \notin S} \mathbf{PGL}_1(\Omega_u)$$

And the same for $\mathbf{SL}_1(\mathbf{B})$.

Let $\mathbf{G} = \mathbf{SL}_1(\mathbf{B})$ or $\mathbf{G} = \mathbf{PGL}_1(\mathbf{B})$. Denote $G_S = \prod_{u \in S} \mathbf{G}(\mathbb{F}_u)$. Let Γ be the arithmetic lattice in G_S associated to Ω . Under the assumptions above

on S we can identify $\Gamma \backslash G^S$ with a factor of the adelic locally homogeneous space $\mathbf{G}(\mathbb{F}) \backslash \mathbf{G}(\mathbb{A})$.

Maximal tori in groups of units in central simple algebras are in bijection with maximal commutative subalgebras of the central simple algebra. In particular, given a homogeneous toral set $Y = \mathbf{G}(\mathbb{F}) \backslash \mathbf{T}(\mathbb{A})g_{\mathbb{A}}$ for each local torus⁴ $\mathbf{H}_u = g_u^{-1} \mathbf{T} g_u$ there is a maximal commutative subalgebra $\mathbf{C}_u < \mathbf{B}_{\mathbb{F}_u}$ such that $\mathbf{H}_u = \mathbf{SL}_1(\mathbf{C}_u)$ or $\mathbf{H}_u = \mathbf{PGL}_1(\mathbf{C}_u)$ accordingly. Let Ω_u be the closure of Ω in $\mathbf{B}(\mathbb{F}_u)$. For a finite place u , the ring $\mathcal{R}_u := \Omega_u \cap \mathbf{C}_u(\mathbb{F}_u)$ is an order in the étale-algebra⁵ $\mathbf{C}_u(\mathbb{F}_u)$. We say the homogeneous toral set is of *maximal type* if \mathcal{R}_u is a maximal order in $\mathbf{C}_u(\mathbb{F}_u)$. This is a generalization of packets associated to maximal orders in number fields.

For simplicity one might just consider the case $\mathbb{F} = \mathbb{Q}$ the rational numbers, $\mathbf{B} = \mathbf{M}_n$ the matrix algebra, $\mathbf{G} = \mathbf{PGL}_n$ the projective linear group, $S = \{\infty\}$ the archimedean place and $\Gamma = \mathbf{PGL}_n(\mathbb{Z})$. In this setting $\Gamma \backslash G^S = \mathbf{PGL}_n(\mathbb{Z}) \backslash \mathbf{PGL}_n(\mathbb{R})$. The split torus which shall be fixed in the Theorem 1.2 can be taken to be the full torus of diagonal matrices. Our theorem is then a result regarding the asymptotic entropy of some packets of periodic orbits for the diagonal action. Notice that in this case one needs to assume non-escape of mass as well.

Theorem 1.2. *Suppose we are given a sequence of homogeneous toral sets of maximal type $Y_i = \mathbf{G}(\mathbb{F}) \backslash \mathbf{T}_i(\mathbb{A})g_i$ with \mathbf{T}_i a torus defined and anisotropic over \mathbb{F} . Denote by D_i the global discriminant of Y_i and let $D_{\text{ram},i}$ be the product of the local discriminants of Y_i at the finite places where \mathbf{B} ramifies. Assume $D_i \rightarrow_{i \rightarrow \infty} \infty$ and $D_{\text{ram},i} = D_i^{o(1)}$.*

Galois Condition: Let \mathbb{L}_i/\mathbb{F} be the splitting field of \mathbf{T}_i . We assume for all i that $\text{Gal}(\mathbb{L}_i/\mathbb{F})$ is 2-transitive.

Splitting Condition: We fix a place $\hat{u} \in S$ such that \mathbf{B} is isotropic over \hat{u} . Denote $\hat{\mathbb{F}} := \mathbb{F}_{\hat{u}}$. Fix a torus $\mathbf{H} < \mathbf{G}_{\hat{\mathbb{F}}}$ defined over $\hat{\mathbb{F}}$ and such that⁶ $\text{rank}_{\hat{\mathbb{F}}} \mathbf{H} > 0$. Set $H = \mathbf{H}(\hat{\mathbb{F}})$. Assume for all i that $\mathbf{H}_{i,\hat{u}} := g_{i,\hat{u}}^{-1} \mathbf{T}_i g_{i,\hat{u}} = \mathbf{H}$, i.e. all the sets Y_i are invariant in the place \hat{u} under a fixed split torus H .

Let μ_i be the probability measure on $\Gamma \backslash G^S$ induced by the probability measure on the homogeneous toral set Y_i . If μ_i converges in the weak- topology to a probability measure μ on $\Gamma \backslash G^S$ then for any $a \in H$ we have⁷*

$$h_{\mu}(a) \geq \frac{h_{\text{Haar}}(a)}{2(n-1)}$$

⁴ g_u is the component of $g_{\mathbb{A}}$ at the place u

⁵An étale-algebra over a field is just finite product of separable field extensions.

⁶The theorem is vacuously true without the splitting assumption for \mathbf{H} .

⁷Evidently, μ must be H -invariant.

Where $h_{\text{Haar}}(a)$ is the entropy of the Haar probability measure on $\Gamma \backslash G_S$, which is the unique measure of maximal entropy.

Remark 1.3. Assume \mathbf{H} is totally split over $\widehat{\mathbb{F}}$ and let Φ be the set of roots for the torus \mathbf{H} . The weaker bound

$$(2) \quad h_{\mu}(a) \geq \frac{1}{2} \min_{\alpha \in \Phi} |\log |\alpha(a)|_{\widehat{u}}|$$

has been proven in [ELMV09][Theorem 3.1] for any $a \in H$ but without any Galois condition or assumption on maximality or ramification. The entropy of the Haar measure is

$$h_{\text{Haar}}(a) = \frac{1}{2} \sum_{\alpha \in \Phi} |\log |\alpha(a)|_{\widehat{u}}|$$

The proof of (2) goes by considering the separation of orbits implied by attaching to the Lie algebra of \mathbf{T}_i an integral point with denominator D_i in $\left(\bigwedge^{\text{rank } \mathbf{G}} \text{Lie}(\mathbf{G})(\mathbb{Q})\right)^{\otimes 2}$. This procedure is essentially the *definition* of the discriminant.

The ability to deduce better bounds using just the adjoint representation on the Lie algebra seems to be limited by the fact that for $\text{rank } \mathbf{G} > 1$ most of the subspaces of dimension $\text{rank } \mathbf{G}$ in $\text{Lie}(\mathbf{G})(\mathbb{Q})$ do not correspond to tori.

Without the condition on the Galois group, our method gives the same entropy bound as in (2). *A key new feature in our paper is that we are able to use additional information about the Galois groups of the splitting fields of the tori to give substantially more precise results.* Moreover, we are able to treat homogeneous toral sets which are invariant under a non totally split torus.

Lets calculate the different available bounds for the case that $\mathbf{G} = \mathbf{PGL}_n$ over \mathbb{Q} , $\widehat{u} = \infty$ – the real place, \mathbf{H} – the standard torus of diagonal matrices and

$$a = \text{diag} \left(\exp \left(\frac{n-1}{2} \right), \exp \left(\frac{n-3}{2} \right), \dots, \exp \left(-\frac{n-1}{2} \right) \right)$$

The roots of \mathbf{H} are parameterized by pairs (i, j) where $1 \leq i \neq j \leq n$. The values of the roots for a as above are

$$\log |\alpha_{i,j}(a)| = j - i$$

In particular

$$\begin{aligned} h_{\text{Haar}}(a) &= \frac{(n+1)n(n-1)}{6} \\ \frac{h_{\text{Haar}}(a)}{2(n-1)} &= \frac{(n+1)n}{12} \\ \frac{1}{2} \min_{\alpha \in \Phi} |\log |\alpha(a)|_{\infty}| &= \frac{1}{2} \end{aligned}$$

A main difference between the bounds is that the new bound grows quadratically with n , unlike the bound (2) which is constant. In conjunction with the measure rigidity results of [EKL06] and [EL15] this implies a new modest qualitative restriction on possible limit measures. Specifically, if $\mathbb{F} = \mathbb{Q}$ then μ is not supported on a single periodic orbit of a reductive group all whose simple parts have small absolute rank compared to \mathbf{G} , see Corollary 9.3.

1.7. An Overview of the Proof. We present a general overview of the proof completely in adelic terms.

Decay of mass for thin tubes. Fix an element $a \in H$. Due to essentially upper semi-continuity of entropy, in order to bound the entropy of the limit measure with respect to a , it is enough to show that the μ_i mass of small tubes in $\mathbf{G}(\mathbb{F}) \backslash \mathbf{G}(\mathbb{A})$ decays exponentially fast with a given rate when these tubes are conjugated by a . Notice that these tubes contract in a single place \hat{u} only.

The rate at which the measure of the contracting tubes decreases is our bound on the entropy with respect to a . For this idea to apply easily we need all our homogeneous toral sets to be invariant under the action of this fixed a . To apply the measure rigidity results of [EKL06] and [EL15] one might need to assume that \mathbf{H} is totally split over $\hat{\mathbb{F}}$.

This method for proving a bound on the entropy is well known and has been used for similar means in [ELMV09] and [ELMV12].

Double torus quotient invariants. Let \mathbf{T} be a rational torus appearing in the series $\{\mathbf{T}_i\}_i$. We construct new polynomial invariants $\Psi_\sigma: \mathbf{G}(\mathbb{F}) \rightarrow \mathbb{L}$ where \mathbb{L}/\mathbb{F} is the splitting field of \mathbf{T} . These invariants depend on \mathbf{T} and we have one such invariant for each σ in the absolute Weyl group of \mathbf{T} . It is useful to choose an identification of the Weyl group with the symmetric group S_n and consider the invariants as parametrized by permutations. The polynomials Ψ_σ are invariant under both the left and the right action of \mathbf{T} .

Application of Geometric invariant theory. Using GIT we are able to prove for two torus cosets $\delta_L \mathbf{T}(\mathbb{A}), \delta_R \mathbf{T}(\mathbb{A})$ with $\delta_L, \delta_R \in \mathbf{G}(\mathbb{F})$ that if for all σ

$$\Psi_\sigma(\delta_L^{-1} \delta_R) = \Psi_\sigma(\text{id})$$

then necessarily $\delta_L \mathbf{T}(\mathbb{A}) = \delta_R \mathbf{T}(\mathbb{A})$.

Arithmetic properties of the invariants. We show that the invariants Ψ_σ satisfy an important arithmetic property. One variant of this result is that for all nonarchimedean places u of \mathbb{F} where \mathbf{B} is unramified we have that if $\delta_L^{-1} \delta_R$ is in an appropriate identity neighborhood in $\mathbf{G}(\mathbb{F}_u)$, i.e. satisfy an integrality condition, then

$$(3) \quad |\text{Nr}_{\mathbb{L}/\mathbb{F}} \Psi_\sigma(\delta_L^{-1} \delta_R)|_u < D_u^{[\mathbb{L}:\mathbb{F}]}$$

Where D_u is the local discriminant of the homogeneous toral set at the place u . Moreover, an analogous result holds in the archimedean places. It is here that we use the maximality assumption for the homogeneous toral set.

Algebraic relations between the invariants and Galois orbits thereof. We exploit two more tools: the algebraic relations between the invariants Ψ_σ for different σ and the action of $\text{Gal}(\mathbb{L}/\mathbb{F})$ on each Ψ_σ . We form a new single invariant $\Psi_\mathcal{C}$ by taking the product of all the Galois conjugates of a specific Ψ_{σ_0} , where σ_0 can be taken as any permutation that has no fixed points. The resulting invariant takes values in the fixed field \mathbb{F} .

Obviously, $\text{Nr}_{\mathbb{L}/\mathbb{F}}\Psi_{\sigma_0}$ is an integral power of $\Psi_\mathcal{C}$ and we can deduce from inequality (3) a similar inequality for $\Psi_\mathcal{C}$.

Under the assumption that $\text{Gal}(\mathbb{L}/\mathbb{F})$ is 2-transitive we are able to combine our understanding of both the Galois orbits of all the invariants Ψ_σ and the algebraic relations between them to show that the equality

$$\Psi_\mathcal{C}(\delta_L^{-1}\delta_R) = 0$$

is enough to deduce that $\Psi_\sigma(\delta_L^{-1}\delta_R) = \Psi_\sigma(\text{id})$ for all $\sigma \in S_n$.

Using the invariants to study thin tubes. At this point we have most of the tools to apply the method described in the first step. We study the value of $\Psi_\mathcal{C}$ on pairs of translated cosets $\delta_L\mathbf{T}(\mathbb{A})g, \delta_R\mathbf{T}(\mathbb{A})g$ that lie in the same thin tube. By choosing our tube carefully in all the places we are able to insure that the integrality conditions required for (3) hold. Hence we have a bound on the absolute value of $\Psi_\mathcal{C}(\delta_L^{-1}\delta_R)$ in every place u in terms of the local discriminant D_u .

Moreover, at the single place \hat{u} where the tube is contracted we can give an exponentially good bound on the \hat{u} absolute value of $\Psi_\mathcal{C}(\delta_L^{-1}\delta_R)$ for pairs of cosets as above. The rate of this exponential bound affects critically the final bound on the entropy. Here we use 2-transitivity of the Galois group again in conjugation with the fact that we chose σ_0 to be without fixed points to optimize this rate.

We multiply the bounds for all the places of \mathbb{F} to have a bound on the adelic norm of $\Psi_\mathcal{C}(\delta_L^{-1}\delta_R)$ in terms of the global discriminant and the exponential decay at the single place. By pushing the exponential bound far enough in comparison with the global discriminant term we can decrease the bound on the norm below 1. But $\Psi_\mathcal{C}(\delta_L^{-1}\delta_R) \in \mathbb{F}$, viz. it is a rational number, hence if it has norm smaller than 1 then it is equal to 0. Combining the previous statements we conclude that a tube which has been contracted long enough must include a single coset at most. This implies immediately a bound on the tube's measure.

1.8. Harmonic Analytic Methods. The splitting condition in Linnik's result about the equidistribution of projections of integral points to the 2-sphere has been removed using analytic number theory by W. Duke about 30 years after Linnik's results.

The analytic methods verify the Weyl equidistribution criterion for a suitable base of $L_0^2(\mathbf{S}^2(\mathbb{R}), m)$. The base is chosen so that the averages of the base functions over integral points can be realized as familiar number theoretic objects. The first proof of unconditional equidistribution for $n = 3$ is due to [Duk88]. Duke uses the theta correspondence to relate the averages of suitable base functions to Fourier coefficients of modular forms; for which he applies bounds he has proved building on the work of Iwaniec [Iwa87].

A second approach from harmonic analysis emerged soon after Duke's proof. It uses Waldspurger's formula [Wal85] to relate the averages of appropriate base functions over integral points to central values of some L -functions. Combined with subconvexity results for these L -functions this leads to a proof of Duke's theorem. The review [MV06] by Michel and Venkatesh provides a concise description of the harmonic analysis arising in the study of this problem and related ones.

1.9. Conditional Results for \mathbf{PGL}_n . In [ELMV11] Einsiedler, Lindenstrauss, Michel and Venkatesh have proven the following theorem by fusing results from harmonic analysis and homogeneous dynamics.

Theorem. *Let $\mathbf{G} = \mathbf{PGL}_n$. Let \mathbf{H} , H , Y_i , μ_i and D_i be as in Theorem 1.2. Denote by Φ the set of roots of \mathbf{H} .*

Subconvexity Hypothesis: For any degree n field extension \mathbb{K}/\mathbb{F} with discriminant $D_{\mathbb{K}}$ assume that a subconvex bound⁸ in the $D_{\mathbb{K}}$ aspect holds for Hecke L -functions associates to \mathbb{K} .

Under this hypothesis the following holds

Non-escape of mass: *The collection $\{\mu_i\}_i$ is tight, i.e. any weak-* limit of a subsequence of $\{\mu_i\}_i$ is a probability measure.*

Entropy bound: *Let μ be any weak-* limit of a subsequence of $\{\mu_i\}_i$. Then for any $a \in H$*

$$(4) \quad h_{\nu}(a) \geq \min_{\alpha \in \Phi} |\log |\alpha(a)|_{\hat{u}}|$$

For ν almost every ergodic component of μ .

Let m be the Haar probability measure on $\Gamma \backslash G_S$. The method of proof for this theorem goes by verifying the Weyl equidistribution criterion for the *Eisenstein series* in $L_0^2(\Gamma \backslash G_S, m)$, which is possible because of a period formula due to Hecke that expresses toral integrals of Eisenstein series using L -functions. It is those L -functions for which subconvexity has to be assumed. A significant part of the proof is bounding additional local contributions arising in the period formula.

Unfortunately, although the pertinent subconvexity bound follows from the GRH, it is unknown unconditionally for $n > 3$. Moreover, the theorem's method of proof can not apply for division algebras where there is no Eisenstein series in $L_0^2(\Gamma \backslash G_S, m)$.

⁸See [ELMV11, Expression (71)] for an exact statement.

Not only does this theorem shows non-escape of mass, when it applies it has a significant advantage over Theorem 1.2 because it insures that *almost every* ergodic component of a limit measure has positive entropy. In particular, this theorem together with [EKL06] and [EL15] implies that any weak-* limit of μ_i must be homogeneous. When n is prime this means that the limit is the unique Haar probability measure. For n not prime there is a serious issue of possible intermediate measures supported on periodic orbits of non-maximal reductive subgroups.

We stress that with the current state of knowledge, even assuming GRH, our result in Theorem 1.2 provides for n not prime *new* information regarding the possible limits of μ_i . This is so because the bound we show for the entropy of a limit measure, which is the average over all ergodic components, is significantly better than the one implied by (4).

1.10. Organization of the paper. In §2, we review the concept of homogeneous toral sets in reductive linear algebraic groups and discuss their volume and discriminant data.

In §3 we construct the double quotient of a reductive linear group by a torus and study elementary properties of the quotient using geometric invariant theory.

In §4 we present the canonical generators for the double quotient of \mathbf{SL}_n and \mathbf{PGL}_n by the maximal diagonal torus and analyze the algebraic relations between them.

In §5 we review the relation between the canonical generators of \mathbf{PGL}_2 and the discriminant inner product used by Linnik and Skubenko.

In §6 we use the results of §4 to construct canonical generators for a general rational torus in the projective or special group of units of a central simple algebra. Notably, we study the Galois orbits of the values of canonical generators.

In §7 we prove arithmetic results relating the denominators of values of canonical generators for central simple algebras with the discriminant data of homogeneous toral sets.

In §8 we show that values of canonical generators decay exponentially in contracting Bowen balls and prove the entropy lower bound.

In §9 we combine the results of §8 with the measure rigidity theorems of [EKL06] and [EL15] to derive a statement about possible limit measures for a sequence of packets.

1.11. Acknowledgments. This paper is part of the author's PhD thesis conducted at the Hebrew University of Jerusalem under the guidance of Prof. E. Lindenstrauss, to whom I am grateful for introducing me to homogeneous dynamics and number theory, and for many helpful discussions and insights. I would like to express my gratitude to Akshay Venkatesh for encouraging and valuable conversations.

Work on this project began during the MSRI program "Geometric and Arithmetic Aspects of Homogeneous Dynamics" in 2015. It is a pleasure

to thank MSRI and the organizers for the program and for the institute's hospitality.

Last but not least, I would like to thank my wife, Olga Kalantarov, for her unconditional support during the preparation of this paper.

The author has been supported by the ERC throughout his PhD studies.

2. THE GENERAL SETTING AND HOMOGENEOUS TORAL SETS

2.1. Algebraic Groups and Adeles. Let \mathbf{G} be a reductive linear algebraic group defined over a number field \mathbb{F} . Our objects of study are collections of periodic orbits of a maximal torus in \mathbf{G} on an S -arithmetic quotient. Following [ELMV11] we describe an arithmetic grouping of periodic torus orbits induced by a single adelic torus.

For each place u of \mathbb{F} denote by \mathbb{F}_u the completion of \mathbb{F} at u . We denote by $\mathcal{V}_{\mathbb{F}}$, $\mathcal{V}_{\mathbb{F},\infty}$ and $\mathcal{V}_{\mathbb{F},f}$ the set of all places on \mathbb{F} , the set of all archimedean places and the set of all nonarchimedean places respectively. For u nonarchimedean we write $|\cdot|_u$ to be the canonical absolute value on \mathbb{F}_u , i.e. $|\varpi|_u = q^{-1}$ where ϖ is a uniformizer for the ring of integers of \mathbb{F}_u and q is the size of the residue field. For u archimedean $|\cdot|_u$ is the standard absolute value on \mathbb{R} or \mathbb{C} .

Let S be a finite set of places of \mathbb{F} including all the infinite ones. Denote by \mathbb{A} the adele ring of \mathbb{F} and let $\mathbb{A}^S \subset \mathbb{A}$ be the set of adeles having zero v -component for each $v \in S$. Set also $\mathbb{F}_S := \prod_{u \in S} \mathbb{F}_u$, then $\mathbb{A} = \mathbb{F}_S \times \mathbb{A}^S$.

We always treat \mathbb{F} as diagonally embedded in \mathbb{A} , \mathbb{A}^S and \mathbb{F}_S . Similarly, for an affine algebraic variety \mathbf{V} defined over \mathbb{F} , we treat $\mathbf{V}(\mathbb{F})$ as diagonally embedded in $\mathbf{V}(\mathbb{A})$ and $\mathbf{V}(\mathbb{F}_S)$. The spaces $\mathbf{V}(\mathbb{A})$ and $\mathbf{V}(\mathbb{F}_S)$ inherit a locally compact Hausdorff topology from the standard topology on \mathbb{A} and \mathbb{F}_S .

For a field extension \mathbb{M}/\mathbb{F} and an algebraic variety \mathbf{V} defined over \mathbb{F} we denote by $\mathbf{V}_{\mathbb{M}}$ the base change of \mathbf{V} to \mathbb{M} . In scheme theoretic language $\mathbf{V}_{\mathbb{M}} := \mathbf{V} \times_{\text{Spec } \mathbb{F}} \text{Spec } \mathbb{M}$. As all the main varieties we deal with are affine ones, the base change can be described completely by the transformation of the ring of regular functions $\mathbb{M}[\mathbf{V}_{\mathbb{M}}] := \mathbb{F}[\mathbf{V}] \otimes_{\mathbb{F}} \mathbb{M}$.

2.2. S -Arithmetic and Adelic Quotients. Denote $G_S := \prod_{u \in S} \mathbf{G}(\mathbb{F}_u)$. We are interested in the locally homogeneous space $X_S := \Gamma \backslash G_S$ for a congruence lattice Γ .

This space can be naturally identified with the identity component of a factor space of the adelic quotient $X := \mathbf{G}(\mathbb{F}) \backslash \mathbf{G}(\mathbb{A})$. To see this fix a compact open subgroup $K_S < \mathbb{A}^S$ such that $\Gamma = \mathbf{G}(\mathbb{F}) \cap K_S$ with the intersection taking place in $\mathbf{G}(\mathbb{A}^S)$. We have the obvious right action of G_S on $X/K_S = \mathbf{G}(\mathbb{F}) \backslash \mathbf{G}(\mathbb{A})/K_S$. By a theorem of Borel, the finiteness of class number, the double quotient $\mathbf{G}(\mathbb{F}) \backslash \mathbf{G}(\mathbb{A})/K_S$ is finite [Bor63, Theorem 5.1] (see also [Con12]). In particular X_S can be identified with the identity component of X/K .

2.3. Homogeneous Toral Sets and Packets. A rational maximal torus in \mathbf{G} is an algebraic subgroup $\mathbf{T} < \mathbf{G}$ defined over \mathbb{F} which is a maximal torus in \mathbf{G} .

The notion of a homogeneous toral set has been defined in [ELMV11, §4.1]. For a given $g_{\mathbb{A}} \in \mathbf{G}(\mathbb{A})$ and a maximal torus $\mathbf{T} < \mathbf{G}$ defined over \mathbb{F} we define the homogeneous toral set to be the following subset of X

$$Y := \mathbf{G}(\mathbb{F}) \backslash \mathbf{T}(\mathbb{A}) g_{\mathbb{A}}$$

If $g_{\mathbb{A}} = (g_u)_{u \in \mathcal{V}_{\mathbb{F}}}$ then for each place u we can define over \mathbb{F}_u the torus $\mathbf{H}_u = g_u^{-1} \mathbf{T}_{\mathbb{F}_u} g_u$. The homogeneous toral set is an orbit of the geometric torus $\mathbf{H}_u(\mathbb{F}_u)$ for each u .

The homogeneous toral set can be identified with $\mathbf{T}(\mathbb{F}) \backslash \mathbf{T}(\mathbb{A})$. If \mathbf{T} is anisotropic over \mathbb{F} then $\mathbf{T}(\mathbb{F})$ is a lattice in $\mathbf{T}(\mathbb{A})$. In particular, $\mathbf{T}(\mathbb{F}) \backslash \mathbf{T}(\mathbb{A})$ carries a unique probability measure invariant under $\mathbf{T}(\mathbb{A})$. This induces a probability measure on Y invariant under the action of $\mathbf{H}_u(\mathbb{F}_u)$ for each u .

We assume hereon that \mathbf{T} is anisotropic over \mathbb{F} .

2.4. Discriminant and Volume. The volume and discriminant of a homogeneous toral set have been defined in [ELMV11, §§4.2–4.3]. We reproduce these definitions here for convenience's sake.

2.4.1. Volume. This definition depends on a fixed pre-compact identity neighborhood $\mathcal{K} \subset \mathbf{G}(\mathbb{A})$. Let $\mu_{\mathbf{T}}$ be the probability measure on $\mathbf{T}(\mathbb{F}) \backslash \mathbf{T}(\mathbb{A})$, then one defines

$$\text{vol}(Y) = \mu_{\mathbf{T}}(t \in \mathbf{T}(\mathbb{A}) \mid g_{\mathbb{A}}^{-1} t g_{\mathbb{A}} \in \mathcal{K})^{-1}$$

The different values of the volume for different sets \mathcal{K} are comparable up to constants depending on these sets only.

It is convenient to choose $\mathcal{K} = \prod_{u \in \mathcal{V}_{\mathbb{F}}} \mathcal{K}_u$ such that $\prod_{u \notin S} \mathcal{K}_u = K_S$.

2.4.2. Discriminant Data. The discriminant data is composed of a local discriminant D_u for each place u of \mathbb{F} . For u nonarchimedean $D_u \in q^{\mathbb{Z}}$ where q is the size of the residue field of \mathbb{F}_u . For u archimedean $D_u \in \mathbb{R}_{>0}$.

Let \mathfrak{g} be the Lie algebra of \mathbf{G} , \mathfrak{t} the Lie algebra of \mathbf{T} and $\mathfrak{h}_u = \text{Ad}(g_u^{-1})\mathfrak{t}$ the Lie algebra of $\mathbf{H}_u = g_u^{-1} \mathbf{T} g_u$. Notice that \mathfrak{h}_u is only defined over \mathbb{F}_u .

Set r to be the absolute rank of \mathbf{G} and let $\mathbf{V} := (\bigwedge^r \mathfrak{g})^{\otimes 2}$. This is an affine space defined over \mathbb{F} . To define the local discriminant we need to make a choice of a good Goldman-Iwahori norm $\|\cdot\|_u$ on $\mathbf{V}(\mathbb{F}_u)$ for all places u . See the discussion at [ELMV11, §7] regarding norms.

These norms must satisfy a compatibility condition which says that for almost all nonarchimedean u the unit ball of the norm coincides with the closure of a fixed $\mathcal{O}_{\mathbb{F}}$ lattice in $\mathbf{V}(\mathbb{F})$.

The subspace $\mathfrak{h}_u(\mathbb{F}_u) < \mathfrak{g}(\mathbb{F}_u)$ defines a point in $\mathbf{V}(\mathbb{F}_u)$ by a variant of the Plücker embedding

$$x_{\mathfrak{h}_u} := (f_1 \wedge \dots \wedge f_r)^{\otimes 2} \cdot \left| \det (B(f_i, f_j))_{1 \leq i, j \leq n} \right|_u^{-1}$$

Where f_1, \dots, f_n is a base for $\mathfrak{h}_u(\mathbb{F}_u)$ and B is the Killing form.

The local discriminant is then defined to be $D_u = \|x_{\mathfrak{h}_u}\|_u$. The global discriminant is $D := \prod_{u \in \mathcal{V}_{\mathbb{F}}} D_u$.

Notice that the local discriminant is a property of \mathbf{H}_u .

Remark 2.1. In many classical cases the archimedean discriminant is uniformly bounded for the homogeneous toral sets in question so it doesn't play a role.

When studying periodic orbits of a fixed split torus \mathbf{H} over \mathbb{R} with $\mathbb{F} = \mathbb{Q}$ as in [ELMV12] or [ELMV09] we have $\mathbf{H}_{\infty} = \mathbf{H}$ and the archimedean discriminant is constant.

When studying the points on the 2-sphere and modular analogues in [Lin68] and [EMV13] all the archimedean tori \mathbf{H}_{∞} in the associated homogeneous toral sets are conjugate through elements of a compact group. Hence the archimedean discriminant is uniformly bounded.

3. GEOMETRIC INVARIANT THEORY OF A DOUBLE QUOTIENT BY A TORUS

In this part we construct and study the double quotient of a reductive linear algebraic \mathbf{G} group by a torus \mathbf{T} . To any two orbits of \mathbf{T} on \mathbf{G} we are able to attach a point on the double quotient space.

The gist of the current section is a characterization of all the pairs of \mathbf{T} -orbits which have the the trivial point attached to them in the double quotient space.

3.1. Preliminaries. Let \mathbf{G} be a reductive linear algebraic group defined over a characteristic 0 field \mathbb{F} and let $\overline{\mathbb{F}}$ be an algebraic closure. Take $\mathbf{T} < \mathbf{G}$ to be a non-trivial torus defined over \mathbb{F} . We always denote by e the identity element of groups when written in multiplicative form.

Recall that for a torus \mathbf{H} defined over \mathbb{F} we can form the character group $X^{\bullet}(\mathbf{H}) = \text{Hom}_{\overline{\mathbb{F}}}(\mathbf{H}, \mathbb{G}_m)$ and the cocharacter group $X_{\bullet}(\mathbf{H}) = \text{Hom}_{\overline{\mathbb{F}}}(\mathbb{G}_m, \mathbf{H})$. Those are free abelian groups whose rank is equal to the absolute rank of \mathbf{H} . The character and cocharacter groups come with a natural perfect pairing $\langle, \rangle : X^{\bullet}(\mathbf{H}) \times X_{\bullet}(\mathbf{H}) \rightarrow \text{End}(\mathbb{G}_m) \simeq \mathbb{Z}$ defined by the composition of a character with a cocharacter. We have an action of the absolute Galois group $\text{Gal}(\overline{\mathbb{F}}/\mathbb{F})$ on $X^{\bullet}(\mathbf{H})$, $X_{\bullet}(\mathbf{H})$ making them Galois modules. In particular $X^{\bullet}(\mathbf{H})^{\text{Gal}(\overline{\mathbb{F}}/\mathbb{F})}$, $X_{\bullet}(\mathbf{H})^{\text{Gal}(\overline{\mathbb{F}}/\mathbb{F})}$ are the groups of characters, respectively cocharacters, defined over \mathbb{F} .

3.2. Synopsis. For convenience's sake we briefly summarize the results of this chapter. The main tools in proving the following statements are the Geometric invariant theory of Mumford [MFK94] and Kempf's work on the numerical criteria for stability of orbits [Kem78].

- (1) There exists an affine algebraic variety defined over \mathbb{F} , $\mathbf{T} \backslash \mathbf{G} // \mathbf{T}$, and an \mathbb{F} -morphism $\pi: \mathbf{G} \rightarrow \mathbf{T} \backslash \mathbf{G} // \mathbf{T}$ which is equivariant with respect to the left and right actions of \mathbf{T} on \mathbf{G} .
- (2) The variety $\mathbf{T} \backslash \mathbf{G} // \mathbf{T}$ can be realised explicitly by choosing a generating set Ψ_1, \dots, Ψ_m in the ring of regular function on \mathbf{G} which are invariant under both the left and the right action of \mathbf{T} . Using the generating functions we define a closed morphism $\Psi = (\Psi_1, \dots, \Psi_m): \mathbf{G} \rightarrow \mathbb{A}^m$. The image of Ψ is isomorphic to $\mathbf{T} \backslash \mathbf{G} // \mathbf{T}$. This isomorphism conjugates Ψ to π .
- (3) For each $\lambda \in \mathbf{G}(\mathbb{F})$ such that $\pi(\lambda) = \pi(e)$ we have $\lambda \in \mathbf{T}(\mathbb{F})$.

The last result is used heavily in what follows. We are able to prove that if two torus orbits $\delta_L \mathbf{T}(\mathbb{A})$ and $\delta_R \mathbf{T}(\mathbb{A})$ with $\delta_L, \delta_R \in \mathbf{G}(\mathbb{F})$ from the same homogeneous toral set come too close to each other then $\pi(\delta_L^{-1} \delta_R) = \pi(e)$. The result quoted above insures us that in this case they must actually be the same orbit. This is exactly the well-separateness property required to prove our entropy inequality.

3.3. Construction and Zariski Closed Orbits. To define the affine algebraic variety $\mathbf{T} \backslash \mathbf{G} // \mathbf{T}$ we start by looking at the action of the algebraic torus $\mathbf{T} \times \mathbf{T}$ on \mathbf{G} defined by $(t_L, t_R).g = t_L g t_R^{-1}$. This is an algebraic action of a reductive algebraic group $\mathbf{T} \times \mathbf{T}$ on an affine algebraic variety \mathbf{G} . Let ${}^{\mathbf{T}}\mathbb{F}[\mathbf{G}]^{\mathbf{T}}$ be the ring of regular function on \mathbf{G} which are invariant under both the left and the right action of \mathbf{T} . By a result of Hilbert this is a finitely generated algebra over \mathbb{F} as $\mathbf{T} \times \mathbf{T}$ is reductive.

The GIT quotient is defined by $\mathbf{T} \backslash \mathbf{G} // \mathbf{T} := \text{Spec } {}^{\mathbf{T}}\mathbb{F}[\mathbf{G}]^{\mathbf{T}}$. This is an affine algebraic variety defined over \mathbb{F} because ${}^{\mathbf{T}}\mathbb{F}[\mathbf{G}]^{\mathbf{T}}$ is finitely generated. This variety comes with a natural $\mathbf{T} \times \mathbf{T}$ -equivariant \mathbb{F} -morphism $\pi: \mathbf{G} \rightarrow \mathbf{T} \backslash \mathbf{G} // \mathbf{T}$ which is induced by the inclusion map ${}^{\mathbf{T}}\mathbb{F}[\mathbf{G}]^{\mathbf{T}} \hookrightarrow \mathbb{F}[\mathbf{G}]$.

The following theorem is a classical result of Mumford's theory for GIT quotients in the affine case.

Theorem 3.1 ([MFK94]). *$\mathbf{T} \backslash \mathbf{G} // \mathbf{T}$ is a universal categorical quotient. In particular the following holds*

- (1) π is surjective.
- (2) Each fibre of π contains a unique Zariski closed orbit.
- (3) For a field extension \mathbb{L}/\mathbb{F} denote by $\mathbf{G}_{\mathbb{L}}$ and $(\mathbf{T} \backslash \mathbf{G} // \mathbf{T})_{\mathbb{L}}$ the corresponding varieties after base change. Then $\mathbf{G}_{\mathbb{L}} \rightarrow (\mathbf{T} \backslash \mathbf{G} // \mathbf{T})_{\mathbb{L}}$ is a categorical quotient for the $\mathbf{T} \times \mathbf{T}$ action.

Proof. See [MFK94, §1.2] and [PV94, §4.4]. □

A significant complication is that the $\mathbf{T} \times \mathbf{T}$ action on \mathbf{G} necessarily has non Zariski closed orbits of $\overline{\mathbb{F}}$ -points. As a consequence this is not a geometric quotient and such a quotient does not exist, at least not for the whole variety \mathbf{G} .

A main tool for studying the Zariski closure of orbits are cocharacters of the acting group $\mathbf{T} \times \mathbf{T}$, also called multiplicative 1-parameter subgroups. Those are morphisms $\mathbb{G}_m \rightarrow \mathbf{T} \times \mathbf{T}$. We cite the following important result of Kempf building upon the work of Mumford and Hilbert (see also [MFK94, Chapter 2]).

Proposition 3.2. [Kem78, Corollary 4.3] *Let \mathbf{H} be a connected reductive algebraic group acting on an affine scheme \mathbf{X} . Let \mathbf{S} be a closed \mathbf{H} -invariant subscheme of \mathbf{X} . Let x be an \mathbb{F} -point of \mathbf{X} and assume that \mathbf{S} meets the Zariski closure of the orbit $\mathbf{H}x$. Then there exists a cocharacter λ of \mathbf{H} defined over \mathbb{F} such that $\mathbf{S} \cap \overline{\mathbf{H}x}^{\text{Zar}}$ contains the \mathbb{F} -point $\lim_{\tau \rightarrow 0} \lambda(\tau)x$.*

Corollary 3.3. [Kem78, Remark, p.314] *If \mathbf{H} has no non-trivial cocharacters defined over \mathbb{F} then the \mathbf{H} -orbit of any \mathbb{F} -point of X is Zariski closed.*

Notice that although the notion of limit in Proposition 3.2 is defined algebraically, because of [Kem78, Lemma 1.2], for an affine algebraic variety X and a local field \mathbb{F} the algebraic definition of the limit coincides with limit in the Hausdorff topology induced from the topology on the field.

Example 3.4. Let $\mathbf{B} = \mathbf{T} \ltimes \mathbf{U}$ be a Borel subgroup defined over $\overline{\mathbb{F}}$ and containing \mathbf{T} and let $n \in N_{\mathbf{G}}(\mathbf{T})(\overline{\mathbb{F}})$. The double torus orbit of $x = nu$ for any $u \in \mathbf{U}(\overline{\mathbb{F}})$, $u \neq e$, is not Zariski closed.

Proof. We will show that n is in the Zariski closure of $\mathcal{O} := \mathbf{T}(\overline{\mathbb{F}})x\mathbf{T}(\overline{\mathbb{F}})$ but $n \notin \mathcal{O}$ because $u \neq e$. This will prove $\overline{\mathcal{O}}^{\text{Zar}} \neq \mathcal{O}$.

Recall that for any Borel subgroup \mathbf{B}' containing the torus \mathbf{T} there is always a cocharacter of \mathbf{T} , $\lambda \in X_{\bullet}(\mathbf{T})$, such that for any character $\alpha \in X^{\bullet}(\mathbf{T})$ we have $\langle \lambda, \alpha \rangle > 0$ if and only if α is a positive character relative to \mathbf{B}' . Let $\lambda \in X_{\bullet}(\mathbf{T})$ be such cocharacter relative to \mathbf{B}^- , i.e. $\langle \lambda, \alpha \rangle < 0$ if and only if α is a positive character relative \mathbf{B} . Now $(n\lambda n^{-1}, \lambda)$ is cocharacter of $\mathbf{T} \times \mathbf{T}$ and

$$(5) \quad \lim_{\tau \rightarrow 0} (n\lambda(\tau)n^{-1}) x \lambda(\tau)^{-1} = n \lim_{\tau \rightarrow 0} [\lambda(\tau)u\lambda(\tau)^{-1}]$$

We claim that $\lim_{\tau \rightarrow 0} [\lambda(\tau)u\lambda(\tau)^{-1}] = e$ as required. To see that use the fact that \mathbf{U} is generated by the 1-parameter unipotent subgroups \mathbf{U}_{α} for positive characters α and decompose u into a product of 1-parameter unipotents. For each 1-parameter unipotent \mathbf{U}_{α} there is an isomorphism $\epsilon_{\alpha} : \mathbb{G}_a \rightarrow \mathbf{U}_{\alpha}$ such that $t\epsilon_{\alpha}(s)t^{-1} = \epsilon_{\alpha}(\alpha(t)s)$ for all $t \in \mathbf{T}(\overline{\mathbb{F}})$ and all $s \in \mathbb{G}_a(\overline{\mathbb{F}})$. In particular for the cocharacter λ it holds $\lambda(\tau)\epsilon_{\alpha}(s)\lambda(\tau)^{-1} = \epsilon_{\alpha}(t^{\langle \lambda, \alpha \rangle} s)$ which tends to 0 for all s if and only if $\langle \lambda, \alpha \rangle < 0$. Hence the claim follows by choosing λ as in (5). \square

In the following we are mainly interested in double torus orbits of rational points $g \in \mathbf{G}(\mathbb{F})$ for a torus \mathbf{T} anisotropic over \mathbb{F} , those points always have Zariski closed double torus orbit.

Proposition 3.5. *Assume \mathbf{T} is anisotropic over \mathbb{F} then the double torus orbit of any $g \in \mathbf{G}(\mathbb{F})$ is Zariski closed.*

Proof. By Corollary 3.3 it is enough to show that $\mathbf{T} \times \mathbf{T}$ has no cocharacter over \mathbb{F} , viz. that the \mathbb{F} -cocharacter group $X_{\bullet}(\mathbf{T} \times \mathbf{T})^{\text{Gal}(\overline{\mathbb{F}}/\mathbb{F})}$ is trivial. This is equivalent to $X_{\bullet}(\mathbf{T})^{\text{Gal}(\overline{\mathbb{F}}/\mathbb{F})}$ being trivial. But for a torus the pairing \langle, \rangle between characters and cocharacters is perfect and Galois equivariant, hence this is the same as \mathbf{T} being anisotropic over \mathbb{F} . \square

3.4. Projections to The Identity. Our argument is going to use only very rudimentary properties of the general theory of double torus quotients. We need only to understand which rational points have the same image in $\mathbf{T} \backslash \mathbf{G} // \mathbf{T}$ as the identity.

Much stronger results can be proved using Galois cohomology about the rational points in the fiber of π over any rational point in the double torus quotient. Unfortunately, difficulties in subsequent parts of the argument, specifically in counting integral points in $\mathbf{T} \backslash \mathbf{G} // \mathbf{T}$, stop us from exploiting such results.

Proposition 3.6. *Assume that \mathbf{T} is anisotropic over \mathbb{F} . Then for any $\lambda \in \mathbf{G}(\mathbb{F})$ such that $\pi(g) = \pi(e)$ we have that $g \in \mathbf{T}(\mathbb{F})$.*

Proof. Proposition 3.5 implies that both $\mathbf{T}g\mathbf{T}$ and $\mathbf{T}e\mathbf{T}$ are Zariski closed. The latter orbit is actually equal to \mathbf{T} .

Theorem 3.1 says that there is a unique Zariski closed orbit over $\pi(e)$, hence $\mathbf{T} = \mathbf{T}e\mathbf{T} = \mathbf{T}g\mathbf{T}$. In particular, over an algebraically closed field $\overline{\mathbb{F}}$ we have $\mathbf{T}(\overline{\mathbb{F}}) = \mathbf{T}(\overline{\mathbb{F}})g\mathbf{T}(\overline{\mathbb{F}})$. That is there exist $t_0, t_L, t_R \in \mathbf{T}(\overline{\mathbb{F}})$ such that

$$t_0 = t_L g t_R^{-1} \implies g = t_L^{-1} t_0 t_R$$

Hence $g \in \mathbf{T}(\overline{\mathbb{F}}) \cap \mathbf{G}(\mathbb{F}) = \mathbf{T}(\mathbb{F})$. \square

4. DOUBLE TORUS QUOTIENT FOR \mathbf{SL}_n AND \mathbf{PGL}_n

Let \mathbb{F} be a number field. We treat the matrix algebra \mathbf{M}_n and the associated linear algebraic groups \mathbf{GL}_n , \mathbf{PGL}_n and \mathbf{SL}_n as defined over \mathbb{F} . We denote by $h: \mathbf{SL}_n \rightarrow \mathbf{PGL}_n$ the standard isogeny between these groups.

4.1. Canonical Generators for Standard Tori. Let $\mathbf{Diag} < \mathbf{M}_n$ be the commutative subalgebra of diagonal matrices and denote $\mathbf{A} = \mathbf{GL}_1(\mathbf{Diag})$. Define $\mathbf{SA} = \mathbf{SL}_1(\mathbf{Diag})$ to be the subgroup of diagonal matrices of determinant 1 and let⁹ $\mathbf{PA} := \mathbf{PGL}_1(\mathbf{Diag})$ to be the full diagonal torus of \mathbf{PGL}_n . Those are maximal tori in the corresponding groups split over \mathbb{F} .

⁹By \mathbf{PGL}_1 of a commutative algebra we always mean the algebra modulo the center of an ambient central simple algebra. It is *not* the trivial space which one would obtain modulo the center of the commutative algebra itself.

We build a specific set of generators for ${}^{\mathbf{PA}}\mathbb{F}[\mathbf{PGL}_n]^{\mathbf{PA}}$ and ${}^{\mathbf{SA}}\mathbb{F}[\mathbf{SL}_n]^{\mathbf{SA}}$ which provides us with a description in coordinates of both $\mathbf{PA}\llbracket\mathbf{PGL}_n\rrbracket\mathbf{PA}$ and $\mathbf{SA}\llbracket\mathbf{SL}_n\rrbracket\mathbf{SA}$.

4.1.1. Double Torus Quotient for the Variety of Matrices. Let \mathbf{M}_n be the affine algebraic variety of $n \times n$ matrices, with $x_{i,j} \in \mathbb{F}[\mathbf{M}_n]$, $1 \leq i, j \leq n$, the function attaching to a matrix its (i, j) entry. In this form the coordinate ring of \mathbf{M}_n is the polynomial algebra $R := \mathbb{F}[x_{i,j}]_{1 \leq i, j \leq n}$. The algebraic group $\mathbf{SA} \times \mathbf{SA}$ acts on \mathbf{M}_n . The first copy of \mathbf{SA} in the product acts by the standard left action and the second copy by the standard right action. The closed embedding $\mathbf{SL}_n \rightarrow \mathbf{M}_n$ is obviously equivariant under this action.

Our first step is to describe $R_0 := {}^{\mathbf{SA}}R^{\mathbf{SA}}$, the ring of regular function on $\mathbf{SA}\llbracket\mathbf{M}_n\rrbracket\mathbf{SA}$. This ring is generated by those polynomials $P \in R$ which are invariant under the $\mathbf{SA} \times \mathbf{SA}$ action.

All the following calculations are executed over an algebraically closed field. When an $n \times n$ matrix is multiplied on the left by $\lambda = \text{diag}(\lambda_1, \dots, \lambda_n)$ and on the right by the inverse of $\mu = \text{diag}(\mu_1, \dots, \mu_n)$ its (i, j) coordinate is multiplied by λ_i/μ_j , i.e. $(\lambda, \mu).x_{i,j} = \lambda_i/\mu_j x_{i,j}$.

A polynomial in $P \in R$ is of the form

$$P = \sum_M b_M \prod_{1 \leq i, j \leq n} x_{i,j}^{M_{i,j}}$$

Where M runs over a finite set of monomials, and $M_{i,j}$ is the power of $x_{i,j}$ in the M -monomial. We identify $M = (M_{i,j})_{1 \leq i, j \leq n}$ with a matrix of non-negative integers. Denote

- $M_i := \sum_{1 \leq j \leq n} M_{i,j}$ - the sum of the columns in row i .
- $M^j := \sum_{1 \leq i \leq n} M_{i,j}$ - the sum of the rows in column j .

We see that the double torus action on P takes the form

$$(\lambda, \mu).P = \sum_M b_M \left(\prod_{1 \leq i \leq n} \lambda_i^{M_i} \right) \left(\prod_{1 \leq j \leq n} \mu_j^{M^j} \right)^{-1} \prod_{1 \leq i, j \leq n} x_{i,j}^{M_{i,j}}$$

In particular the $\mathbf{SA} \times \mathbf{SA}$ actions sends monomials to monomials. If the polynomial P is invariant, then because the polynomial algebra is free and the action conserves monomials we must have that each monomial appearing in P is invariant. This implies that R_0 is generated by invariant monomials. For such an invariant monomial with power matrix M we must have for all diagonal matrices λ, μ with determinant 1

$$(6) \quad \left(\prod_{1 \leq i \leq n} \lambda_i^{M_i} \right) \left(\prod_{1 \leq j \leq n} \mu_j^{M^j} \right)^{-1} = 1$$

The only relation between the λ_i 's is $\prod_{1 \leq i \leq n} \lambda_i = 1$ and the same hold for the μ_j 's. Equality (6) can hold if and only if for all $1 \leq i_1, i_2 \leq n$:

$M_{i_1} = M_{i_2}$ and for all $1 \leq j_1, j_2 \leq n$: $M^{j_1} = M^{j_2}$. A matrix M of non-negative integers all whose rows sum to the same value and all whose columns sum to the same value is called a semi-magic square. Notice that because $\sum_{1 \leq i \leq n} M_i = \sum_{1 \leq j \leq n} M^j$ the value must be the same for the rows and the columns.

It is a classical result of D. König that each semi-magic square is a sum of permutation matrices [Kön16] (see also the exposition [LM99]). An immediate consequence is that R_0 is generated by the monomials corresponding to permutation matrices. The discussion above sums to the proof of the following.

Proposition 4.1. *The ring $R_0 = {}^{\mathbf{SA}}\mathbb{F}[\mathbf{M}_n]^{\mathbf{SA}}$ is generated by the monomials*

$$\Psi_\sigma^0 := \text{sign } \sigma \prod_{1 \leq i \leq n} x_{\sigma(i), i}$$

for $\sigma \in S_n$.

Remark 4.2. There are many relations between these generators. In particular notice that we have $n!$ generators, but ${}^{\mathbf{SA}}\mathbb{M}_n//{}^{\mathbf{SA}}$ has a Zariski open subset of dimension $n^2 - 2(n - 1)$. This is the set of stable points - the points that have a Zariski closed orbit and trivial stabilizer. Nevertheless, R_0 is finitely presented and we can describe all the relations explicitly.

4.1.2. *Passing from \mathbf{M}_n to \mathbf{SL}_n .* We recall the definition of the determinant using the Leibniz formula

$$\det := \sum_{\sigma \in S_n} \text{sign } \sigma \cdot \prod_{i=1}^n x_{\sigma(i), i} = \sum_{\sigma \in S_n} \Psi_\sigma^0 \in R$$

This is a homogeneous polynomial of degree n . Denote by $I := \langle \det - 1 \rangle$ the principal ideal in R generated by $\det - 1$. The definition of the special linear group implies $\mathbb{F}[\mathbf{SL}_n] = R/I$.

We are interested in the ring of invariants $\left(R/I\right)_0 := {}^{\mathbf{SA}}\left(R/I\right)^{\mathbf{SA}}$. Define $I_0 := I \cap R_0$. We have an injective homomorphism of \mathbb{F} -algebras $R_0/I_0 \hookrightarrow \left(R/I\right)_0$. The following lemma which appears in the work of Nagata [Nag64, Lemma 5.1.A] implies that this homomorphism is actually an isomorphism (see also [Dol03, Lemma 3.5]).

Lemma 4.3 (Nagata). *Let a linearly reductive algebraic group \mathbf{H} act on the \mathbb{F} -algebras S and S' for a field \mathbb{F} . Assume everything is defined over \mathbb{F} . If $\phi: S \rightarrow S'$ is an \mathbf{H} -equivariant \mathbb{F} -homomorphism **onto** S' , then induced homomorphism $S^{\mathbf{H}} \rightarrow S'^{\mathbf{H}}$ is onto.*

Corollary 4.4. *The homomorphism $R_0/I_0 \hookrightarrow \left(R/I\right)_0$ is an isomorphism. This allows us to identify hereon $R_0/I_0 \simeq \left(R/I\right)_0$.*

In particular $\left(R/I\right)_0$ is generated by $\{\Psi_\sigma^0 \mid \sigma \in S_n\}$ and we can describe $\mathbf{SA} \parallel \mathbf{SL}_n \parallel \mathbf{SA}$ in coordinate form by the image of $\Psi: \mathbf{SL}_n \rightarrow \mathbb{A}^{(n!)}$ defined by $\Psi = (\Psi_\sigma^0)_{\sigma \in S_n}$ where we have fixed an arbitrary order on S_n .

Proof. Applying the lemma to the homomorphism $R \rightarrow R/I$ shows that the homomorphism $R_0 \rightarrow \left(R/I\right)_0$ is onto, but this homomorphism factors through R_0/I_0 . This shows that $R_0/I_0 \rightarrow \left(R/I\right)_0$ is bijective hence an isomorphism. \square

4.1.3. *Passing from \mathbf{SL}_n to \mathbf{PGL}_n .* The isogeny $h: \mathbf{SL}_n \rightarrow \mathbf{PGL}_n$ restricts to an isogeny of maximal tori $h|_{\mathbf{SA}}: \mathbf{SA} \rightarrow \mathbf{PA}$. Using h we can let $\mathbf{SA} \times \mathbf{SA}$ act on the affine algebraic variety \mathbf{PGL}_n to form the double quotient $\mathbf{SA} \parallel \mathbf{PGL}_n \parallel \mathbf{SA}$. Surjectivity of $h|_{\mathbf{SA}}$ implies that

$$\mathbf{SA} \parallel \mathbf{PGL}_n \parallel \mathbf{SA} = \mathbf{PA} \parallel \mathbf{PGL}_n \parallel \mathbf{PA}$$

From now on we identify those spaces.

Next we use the surjectivity of the full isogeny h . The morphism h induces a surjective morphism $\mathbf{SA} \parallel \mathbf{SL}_n \parallel \mathbf{SA} \rightarrow \mathbf{PA} \parallel \mathbf{PGL}_n \parallel \mathbf{PA}$. This morphism intertwines the \mathbf{SA} actions and it is the unique morphism having this property, as follows from the categorical properties of the quotient.

Because of the duality between affine algebraic varieties over \mathbb{F} and finitely generated reduced algebras over \mathbb{F} we have an *injective* algebra homomorphism

$$\mathbf{PA} \mathbb{F}[\mathbf{PGL}_n]^{\mathbf{PA}} \hookrightarrow \mathbf{SA} \mathbb{F}[\mathbf{SL}_n]^{\mathbf{SA}}$$

In particular, if one can demonstrate a set of elements in $\mathbf{PA} \mathbb{F}[\mathbf{PGL}_n]^{\mathbf{PA}}$ whose image in $\mathbf{SA} \mathbb{F}[\mathbf{SL}_n]^{\mathbf{SA}}$ generates the latter ring, then those elements must generate the former ring. We will find such regular functions on \mathbf{PGL}_n that are equal to the Ψ_σ^0 's when restricted to the image of \mathbf{SL}_n .

To represent \mathbf{PGL}_n as an affine algebraic variety we use the adjoint representation which is a closed immersion $\mathbf{PGL}_n \rightarrow \mathbf{GL}_n(\mathbf{M}_n)$. Notably, every regular function on $\mathbf{GL}_n(\mathbf{M}_n)$ induces a regular function on \mathbf{PGL}_n . Hence, all we need to do is to exhibit regular functions on $\mathbf{GL}_n(\mathbf{M}_n)$ such that when restricted to the image of \mathbf{SL}_n through the adjoint representation they would be equal to the Ψ_σ^0 's.

This is easy enough to do if we rewrite Ψ_σ in a slightly more intrinsic way. For $1 \leq i \leq n$ let $e_i^0 = \text{diag}(0, \dots, 0, 1, 0, \dots, 0)$ be the diagonal matrix with a single 1 entry in the (i, i) place. Then for $g \in \mathbf{SL}_n(\overline{\mathbb{F}})$

$$\Psi_\sigma^0(g) = \det \left(\sum_{i=1}^n e_{\sigma(i)}^0 g e_i^0 \right) = \det \left(\sum_{i=1}^n e_{\sigma(i)}^0 \text{Ad}_g(e_i^0) \right)$$

The latter expression can be easily extended to a regular function on the variety $\mathbf{GL}_n(\mathbf{M}_n)$ by considering a general linear transformation on \mathbf{M}_n instead

of Ad_g . Those regular functions would necessarily generate ${}^{\text{PA}}\mathbb{F}[\mathbf{PGL}_n]^{\text{PA}}$ as required. We sum up these results in the following proposition.

Proposition 4.5. *The ring ${}^{\text{PA}}\mathbb{F}[\mathbf{PGL}_n]^{\text{PA}}$ is generated by the following regular functions, which by abuse of notation we also denote by Ψ_σ^0*

$$(7) \quad \Psi_\sigma^0(g) = \det \left(\sum_{i=1}^n e_{\sigma(i)}^0 \text{Ad}_g(e_i^0) \right) = \det \left(\sum_{i=1}^n e_{\sigma(i)}^0 g e_i^0 \right) \cdot (\det g)^{-1}$$

For any $g \in \mathbf{PGL}_n(\overline{\mathbb{F}})$ and all $\sigma \in S_n$. In expression (7) we have treated g as a matrix representing a point in \mathbf{PGL}_n .

Notice that by choosing a representative of determinant 1 we recover the standard polynomials Ψ_σ^0 on \mathbf{SL}_n . Such a representative does not necessarily exist in a field but it always exists over an algebraic closure.

Moreover, the homomorphism ${}^{\text{PA}}\mathbb{F}[\mathbf{PGL}_n]^{\text{PA}} \hookrightarrow \mathbf{SA}\mathbb{F}[\mathbf{SL}_n]^{\text{SA}}$ is an isomorphism of \mathbb{F} -algebras, i.e. $\mathbf{SA}\mathbb{F}[\mathbf{SL}_n]^{\text{SA}} \cong \mathbf{PA}\mathbb{F}[\mathbf{PGL}_n]^{\text{PA}}$. In particular, the relations between the Ψ_σ^0 's for \mathbf{PGL}_n are the same as for \mathbf{SL}_n .

From now on, unless stated otherwise, we write the $(\det g)^{-1}$ factor and its analogues even when treating \mathbf{SL}_n . In that case it should be viewed as the constant function 1. In any case, we can always consider the functions Ψ_σ^0 as functions on \mathbf{GL}_n .

4.2. Relations between the Canonical Generators. We present two different results regarding the relations between the canonical generators. The first one is specially adapted to our needs and is restricted to the question of when one canonical generator being equal to zero implies that another generator is also zero. In the second part we describe explicitly a complete set of relations between the generators.

Proposition 4.6. *To each $\sigma \in S_n$ we attach the **roots set** ¹⁰*

$$R_\sigma := \{(\sigma(i), i) \mid 1 \leq i \leq n, \sigma(i) \neq i\}$$

We say that a subset $\mathcal{C} \subseteq S_n$ has a complete set of roots if

$$\bigcup_{\sigma \in \mathcal{C}} R_\sigma = \{(j, i) \mid 1 \leq j, i \leq n, i \neq j\}$$

Notice that if $F < S_n$ is a 2-transitive subgroup then for every $\sigma \neq \text{id}$ the subset $\{\tau\sigma\tau^{-1} \mid \tau \in F\}$ has a complete set of roots.

If for $g \in \mathbf{GL}_n(\mathbb{F})$ there exists $\sigma \in S_n$ such that σ has no fixed points and $\Psi_\sigma^0(g) = 0$ then in every subset $\mathcal{C} \subseteq S_n$ which has a complete set of roots one can find $\tau \in \mathcal{C}$ such that $\Psi_\tau^0(g) = 0$.

Proof. Lets write g in matrix form $(g_{i,j})_{1 \leq i,j \leq n}$, viz. $x_{i,j}(g) = g_{i,j}$. Recall that $\Psi_\sigma^0(g) := \text{sign } \sigma \prod_{1 \leq i \leq n} g_{\sigma(i), i} \cdot (\det g)^{-1}$. Hence if $\Psi_\sigma^0(g) = 0$ then there exists $1 \leq i_0 \leq n$ such that $g_{\sigma(i_0), i_0} = 0$ and $\sigma(i_0) \neq i_0$.

¹⁰The connection to the roots of a maximal torus in an algebraic group is presented in §8.

For every $\tau \in S_n$ such that $\tau(i_0) = \sigma(i_0)$ we have $\Psi_\tau^0(g) = 0$. In every subset $\mathcal{C} \subseteq S_n$ that has a complete set of roots one can find such $\tau \in \mathcal{C}$ and the proposition follows. \square

4.2.1. Complete Description of the Relations. The results in the second part of this section are presented mainly for the sake of completeness as they do not play a direct role in what follows. Nevertheless, the relations between the generators are a key part of our argument albeit only in the form of Proposition 4.6 and not in the explicit form presented here.

Renormalization of the canonical generators. We wish first to describe the relations between the canonical generators in $R_0 = \mathbf{SA}\mathbb{F}[\mathbf{M}_n]\mathbf{SA}$. Here we work with a different normalization for generators of R_0

$$(8) \quad \Psi_\sigma^1 = \prod_{i=1}^n x_{i,\sigma(i)} = \prod_{1 \leq i,j \leq n} x_{i,j}^{P_{i,j}^\sigma}$$

Where $P^\sigma \in \mathbf{M}_n(\mathbb{Z})$ is the standard permutation matrix associated to $\sigma \in S_n$. Notice the lack of the twist by the determinant as currently we just study R_0 .

We can easily recover the original canonical generators from Proposition 4.1 using $\Psi_\sigma^0 = \text{sign } \sigma \Psi_{\sigma^{-1}}^1$.

The composition map. Any possible relation can be expressed as

$$Q(\Psi_\sigma^1)_{\sigma \in S_n} = 0$$

for a polynomial $Q \in \mathbb{F}[y_\sigma]_{\sigma \in S_n}$ with $\{y_\sigma\}_{\sigma \in S_n}$ formal variables.

We can define the composition map $C_\Psi: \mathbb{F}[y_\sigma]_{\sigma \in S_n} \rightarrow R = \mathbb{F}[\mathbf{M}_n]$ for any polynomial $Q \in \mathbb{F}[y_\sigma]_{\sigma \in S_n}$ by $C_\Psi(Q) = Q(\Psi_\sigma^1)_{\sigma \in S_n}$. This composition is an element of R_0 and hence an element of R . This map is an \mathbb{F} -homomorphism between \mathbb{F} -algebras. The relations in the ring R_0 correspond to $\ker C_\Psi$ which is an ideal of $\mathbb{F}[y_\sigma]_{\sigma \in S_n}$. By Hilbert's Basis Theorem $\ker C_\Psi$ is finitely generated, hence R_0 is finitely presented. We now turn to describe explicitly a set of generating relations.

Reduction to monomials. Because all the polynomials Ψ_σ^1 for $\sigma \in S_n$ are monomials we have that C_Ψ maps monomials to monomials. Each $Q \in \ker C_\Psi$ can be written in the following form

$$(9) \quad Q = \sum_{P \in \text{Monomials}(R)} \sum_{S \in C_\Psi^{-1}(P)} b_S S$$

Where we have grouped all the monomials appearing in Q by their C_Ψ -image in R .

Because R is a free polynomial algebra $C_\Psi(Q) = 0$ if and only if

$$\sum_{S \in C_\Psi^{-1}(P)} b_S P = 0$$

for each P appearing in the decomposition of Q in (9). This is the same as $\sum_{S \in C_\Psi^{-1}(P)} b_S = 0$ for each such P . Hence $\ker C_\Psi$ is generated by elements of the form $Q = \sum_{S \in C_\Psi^{-1}(P)} b_S S$ for a fixed monomial $P \in R$ with $\sum_{S \in C_\Psi^{-1}(P)} b_S = 0$.

We consider $(b_S)_S$ as a vector in the vector space $\mathbb{F}^{C_\Psi^{-1}(P)}$. This vector is contained in the subspace of vectors whose sum is zero. This subspace is spanned by vectors with a single $+1$ entry and a single -1 and the rest of the entries equal to 0. Thus $\ker C_\Psi$ is generated by elements of the form $S_1 - S_2$ for two monomials in $\mathbb{F}[y_\sigma]_{\sigma \in S_n}$ such that $C_\Psi(S_1) = C_\Psi(S_2)$.

Translation to permutation matrices. Let $S_1, S_2 \in \mathbb{F}[y_\sigma]_{\sigma \in S_n}$ be two monomials. Write $S_1 = \prod_{\sigma \in S_n} y_\sigma^{a_\sigma}$ and $S_2 = \prod_{\sigma \in S_n} y_\sigma^{b_\sigma}$. Then $C_\Psi(S_1) = C_\Psi(S_2)$ if and only if

$$\sum_{\sigma \in S_n} (a_\sigma - b_\sigma) P^\sigma = 0$$

Let $c_\sigma = a_\sigma - b_\sigma$ and define $a_\sigma^0 := \max(c_\sigma, 0)$ and $b_\sigma^0 := \max(-c_\sigma, 0)$ for all $\sigma \in S_n$. Let $S_1^0 = \prod_{\sigma \in S_n} y_\sigma^{a_\sigma^0}$ and $S_2^0 = \prod_{\sigma \in S_n} y_\sigma^{b_\sigma^0}$. Evidently $C_\Psi(S_1^0) = C_\Psi(S_2^0)$. Moreover, if $\langle S_1^0 - S_2^0 \rangle$ is the ideal in $\mathbb{F}[y_\sigma]_{\sigma \in S_n}$ generated by $S_1^0 - S_2^0$ then $S_1 - S_2 \in \langle S_1^0 - S_2^0 \rangle$.

To sum up, the ideal $\ker C_\Psi$ is generated by elements of the form $S_f^+ = \prod_{\sigma \in S_n} y_\sigma^{\max(f(\sigma), 0)}$ and $S_f^- = \prod_{\sigma \in S_n} y_\sigma^{\max(-f(\sigma), 0)}$ for any function $f: S_n \rightarrow \mathbb{Z}_{\geq 0}$ such that

$$(10) \quad \sum_{\sigma \in S_n} f(\sigma) P^\sigma = 0$$

The group algebra of S_n . The group ring $\mathbb{Z}S_n$ consists of all function $S_n \rightarrow \mathbb{Z}$, it is an order in the group algebra $\mathbb{Q}S_n$ which consists of all the functions $S_n \rightarrow \mathbb{Q}$. All the irreducible representation of S_n in characteristic zero are defined over \mathbb{Q} . Moreover, they can be defined over \mathbb{Z} , i.e. they are representations of the form $S_n \rightarrow \mathbf{GL}_k(\mathbb{Z})$.

If (ρ, W) is a representation of S_n defined over \mathbb{Q} we have the Fourier transform of any $f \in \mathbb{Q}S_n$ defined by

$$\widehat{f}(\rho) = \sum_{\sigma \in S_n} f(\sigma) \cdot \rho(\sigma) \in \text{End}_{\mathbb{Q}}(W)$$

Let $\rho_0 = \rho_{\text{St}} \oplus \rho_{\text{triv}}$ be the direct sum of the standard representation of S_n with the trivial representation. This is just the representation $\sigma \rightarrow P^\sigma \in \mathbf{GL}_n(\mathbb{Z})$ written as a sum of irreducible representations. Condition (10) can be translated to $\widehat{f}(\rho_0) = 0$.

Let $\{(\rho_i, W_i)\}_i$ be the irreducible representation of S_n defined over \mathbb{Z} . The Fourier transform induces an isomorphism $\mathbb{Q}S_n \xrightarrow{\sim} \bigoplus_i \text{End}_{\mathbb{Q}}(W_i)$. By the Plancherel formula for the finite Fourier transform condition (10) becomes the statement that f is orthogonal to the representations $\rho_{\text{St}}, \rho_{\text{triv}}$.

The discussion above constitutes the proof of the following proposition.

Proposition 4.7. *The ring ${}^{\mathbf{SA}}\mathbb{F}[\mathbf{M}_n]^{\mathbf{SA}}$ is generated by the polynomials $\{\Psi_\sigma^1\}_{\sigma \in S_n}$. A complete list of relations may be computed in the following way.*

For each irreducible representation (W, ρ) other than ρ_{St} and ρ_{triv} we look at $\text{End}_{\mathbb{Q}}(W)$ as a subspace of $\mathbb{Q}S_n$. Let $f_1^\rho, \dots, f_{\dim W}^\rho$ be a primitive base for the lattice $\mathbb{Z}S_n \cap \text{End}_{\mathbb{Q}}(W)$. Then each base vector defines a relation

$$\prod_{\sigma \in S_n} (\Psi_\sigma^1)^{\max(f_i^\rho(\sigma), 0)} = \prod_{\sigma \in S_n} (\Psi_\sigma^1)^{\max(-f_i^\rho(\sigma), 0)}$$

Remark 4.8. Notice that the dimension of the maximal component of ${}^{\mathbf{SA}}\mathbb{M}_n//{}^{\mathbf{SA}}\mathbb{M}_n$ is $n^2 - (n-1) - (n-1) = n^2 - 2n + 2$. We have $|S_n| = n!$ generators for the ring and the amount of relations is $\dim \mathbb{Q}S_n - \dim \rho_{\text{St}}^2 - \dim \rho_{\text{triv}}^2 = n! - (n-1)^2 - 1$. The difference between the amount of generators and the amount of relations is $|S_n| - [\dim \mathbb{Q}S_n - \dim \rho_{\text{St}}^2 - \dim \rho_{\text{triv}}^2] = n^2 - 2n + 2$ which is equal to the above mentioned dimension.

Corollary 4.9. *The ring ${}^{\mathbf{SA}}\mathbb{F}[\mathbf{SL}_n]^{\mathbf{SA}}$ is generated by the regular functions $\{\Psi_\sigma^1\}_{\sigma \in S_n}$ from the Proposition 4.7 with the same relations and the additional Leibniz relation*

$$\sum_{\sigma \in S_n} \text{sign } \sigma \Psi_\sigma^1 = 1$$

Proof. This follows from Proposition 4.7 and 4.4. □

5. DOUBLE TORUS QUOTIENT FOR \mathbf{PGL}_2

In this part we demonstrate the connection between the canonical generators of $\mathbf{PA} // \mathbf{PGL}_2 // \mathbf{PA}$ over $\mathbb{F} = \mathbb{Q}$ and the discriminant inner product of integral binary quadratic forms. This section is not formally required for the development of our results, yet it serves as a motivation to the study of the double quotient of a group by a torus. Moreover, we stress some inherent differences between \mathbf{PGL}_2 and higher rank cases.

The action of \mathbf{PGL}_2 on the space of binary quadratic forms and its relation to class groups of quadratic fields is very well known and goes back to Gauss and Dirichlet. This is an extremely rich subject. We present a very concise introduction suited to our needs.

A close variant of this action has been exploited by Linnik to prove his result regarding equidistribution of integral points in the 2-sphere. A central tool in his method is the study of inner product between two forms.

5.1. Binary Quadratic Forms and the Adjoint Action. We denote by \mathcal{Q} the space of binary quadratic forms. The action of \mathbf{PGL}_2 on \mathcal{Q} is induced from the action of \mathbf{GL}_2 on 2-vectors

$$g \cdot q(x, y) = \frac{1}{\det g} q((x, y)g)$$

Denote the Lie algebra of \mathbf{PGL}_2 by \mathfrak{pgl}_2 . We identify \mathfrak{pgl}_2 with \mathbf{M}_2^0 the space of 2×2 trace free matrices. One can define in the following way an

isomorphism over \mathbb{Q} between the adjoint representation of \mathbf{PGL}_2 on \mathfrak{pgl}_2 and the representation of \mathbf{PGL}_2 on the space of binary quadratic forms

$$(11) \quad ax^2 + bxy + cy^2 \mapsto \begin{pmatrix} b & -2a \\ 2c & -b \end{pmatrix}$$

Being an isomorphism of representations it intertwines the action of \mathbf{PGL}_2 on binary quadratic forms with the adjoint action on the Lie algebra.

The ring of invariants for the adjoint action of \mathbf{PGL}_2 on \mathfrak{pgl}_2 is generated by a single invariant, the determinant of the matrix. This is an instance of Chevalley's restriction theorem. The pullback of the determinant under the isomorphism of \mathfrak{pgl}_2 with \mathcal{Q} is a multiple of the discriminant of a binary quadratic form. Specifically, we have an isomorphism of quadratic spaces

$$(\mathcal{Q}, \text{disc}) \longleftrightarrow (\mathfrak{pgl}_2, -\det)$$

5.2. Stabilizers of a Binary Quadratic Form. The stabilizer in \mathbf{PGL}_2 of a non-degenerate *rational* binary quadratic form q is the centralizer of a non-trivial regular element in $\mathfrak{pgl}_2(\mathbb{Q})$, hence it is a maximal torus \mathbf{T} defined over \mathbb{Q} .

The torus \mathbf{T} is anisotropic over \mathbb{Q} if and only if q is irreducible over \mathbb{Q} . Moreover it is split over \mathbb{R} if and only if q is reducible over \mathbb{R} , i.e. $\text{disc}(q) > 0$.

The correspondence between homothety classes of non-degenerate rational binary quadratic forms¹¹ and rational maximal tori is a bijection. We have already seen how to attach a rational maximal torus to a quadratic form in a way which is obviously invariant under homothety. In the other direction, for a maximal rational torus \mathbf{T} its Lie algebra $\mathfrak{t}(\mathbb{Q})$ is a rational subspace of $\mathfrak{g}(\mathbb{Q})$. Using the isomorphism (11) this corresponds to a homothety class of rational quadratic forms. It is straight forward to see that these maps are inverse to each other. For example, the standard diagonal torus corresponds to the homothety class of $q_0(x, y) = xy$.

5.3. Canonical Generators for \mathbf{PA} in \mathbf{PGL}_2 . Denote by \mathfrak{a} the Lie algebra of the maximal torus $\mathbf{PA} < \mathbf{PGL}_2$. The Weyl group of \mathbf{PA} consists of two elements: the identity element, $+1$, which acts trivially on \mathfrak{a} and the element -1 which acts by negation on \mathfrak{a} .

From our study in the previous parts we learn that the canonical generators for $\mathbf{PA} \backslash \mathbf{PGL}_2 / \mathbf{PA}$ are Ψ_{+1} and Ψ_{-1} . The algebra of invariants for the double torus quotient is generated by those polynomials and they are related by a single relation coming from the Leibniz formula

$$\Psi_{+1} + \Psi_{-1} = 1$$

In particular, the algebra of invariants is ${}^{\mathbf{PA}}\mathbb{Q}[\mathbf{PGL}]^{\mathbf{PA}} \cong \mathbb{Q}[\Psi_{+1}]$, i.e. the double quotient space is just a one dimensional affine space.

¹¹Rational forms q and q' are homothetic if $\exists \alpha \in \mathbb{Q}^\times$ such that $q = \alpha q'$.

If we look at the definition of the canonical generators at Proposition 4.1 adding the twist by the determinant for \mathbf{PGL}_2 we see that

$$\Psi_{+1} \left[\begin{pmatrix} a & b \\ c & d \end{pmatrix} \right] = \frac{1}{ad-bc} ad \quad \Psi_{-1} \left[\begin{pmatrix} a & b \\ c & d \end{pmatrix} \right] = -\frac{1}{ad-bc} bc$$

5.4. Canonical Generators for a rational torus in \mathbf{PGL}_2 . Let now $\mathbf{T} < \mathbf{PGL}_2$ be any maximal torus defined over \mathbb{Q} . Let \mathbb{L}/\mathbb{Q} be the splitting field of \mathbf{T} , either $\mathbb{L} = \mathbb{Q}$ and then $\mathbf{T} = \mathbf{PA}$ or \mathbb{L} is a quadratic extension of \mathbb{Q} and then \mathbf{T} is anisotropic over \mathbb{Q} . In both cases \mathbf{T} is conjugate to \mathbf{PA} by an element of $\mathbf{PGL}_2(\mathbb{L})$.

We are going now to construct generators for ${}^{\mathbf{T}}\mathbb{L}[\mathbf{PGL}_2]^{\mathbf{T}}$ from the functions Ψ_{+1} and Ψ_{-1} . This is a simple instance of the construction we carry out in Proposition 6.2.

As \mathbf{T} is \mathbb{L} -split there exists $g \in \mathbf{PGL}_2(\mathbb{L})$ such that $\mathbf{T}_{\mathbb{L}} = \text{Ad}_g \mathbf{PA}_{\mathbb{L}}$. This equality defines uniquely the coset of g in $\mathbf{PGL}_2(\mathbb{L})/N_{\mathbf{PGL}_2}(\mathbf{PA})(\mathbb{L})$. We define

$$\Psi_{\pm 1}^{\mathbf{T}} := \Psi_{\pm 1} \circ \text{Ad}_{g^{-1}}$$

One easily sees by direct computation that $\Psi_{+1}^{\mathbf{T}}$ and $\Psi_{-1}^{\mathbf{T}}$ are invariant under the left and right action of $\mathbf{T}_{\mathbb{L}}$ and that the definition does not depend on the choice of g up to permuting the two generators.

More so, the map $P \mapsto P \circ \text{Ad}_{g^{-1}}$ defines an isomorphism of \mathbb{L} algebras $\mathbf{PA}_{\mathbb{L}}[\mathbf{PGL}_2]^{\mathbf{PA}} \rightarrow {}^{\mathbf{T}}\mathbb{L}[\mathbf{PGL}_2]^{\mathbf{T}}$. If $\mathbb{L} \neq \mathbb{Q}$ this isomorphism is a priori not defined over \mathbb{Q} as $g \notin \mathbb{Q}$. Yet it implies that $\Psi_{+1}^{\mathbf{T}}$ and $\Psi_{-1}^{\mathbf{T}}$ generate the whole ring of left and right $\mathbf{T}_{\mathbb{L}}$ -invariant regular functions over \mathbb{L} .

What we show in the next section is that although $\Psi_{+1}^{\mathbf{T}}$ and $\Psi_{-1}^{\mathbf{T}}$ are defined initially over \mathbb{L} , for any rational point $\lambda \in \mathbf{PGL}_2(\mathbb{Q})$ one has that $\Psi_{\pm 1}^{\mathbf{T}}(\lambda) \in \mathbb{Q}$. Moreover, these functions are actually defined over \mathbb{Q} .

Unfortunately, this is *no more true* for higher rank groups. Nevertheless, an analogous statement, Proposition 6.4, regarding the orbits of the canonical generators under the Galois group $\text{Gal}(\mathbb{L}/\mathbb{Q})$ still holds.

5.5. Discriminant Inner Product. We have a natural invariant for the \mathbf{PGL}_2 action on \mathcal{Q} which is the discriminant. Being a quadratic form it is associated to a bilinear form on \mathcal{Q} which is its polarization. We call this bilinear form the discriminant inner product¹². For two binary quadratic forms this inner product is evaluated by

$$\langle ax^2 + bxy + cy^2, a'x^2 + b'xy + c'y^2 \rangle_{\text{disc}} = bb' - 2ac' - 2a'c$$

Proposition 5.1. *Let $q_{\mathbf{T}}(x, y)$ be a quadratic form of discriminant 1 corresponding to the rational torus $\mathbf{T} < \mathbf{PGL}_2$. Let $\delta \in \mathbf{G}(\mathbb{C})$ then*

$$(\det \delta)^{-1} \langle q_{\mathbf{T}}, \delta \cdot q_{\mathbf{T}} \rangle_{\text{disc}} = \Psi_{+1}^{\mathbf{T}}(\delta) - \Psi_{-1}^{\mathbf{T}}(\delta)$$

¹²Notice that it is not positive definite yet it is non-degenerate.

Proof. First notice that the polynomial map $\delta \mapsto (\det \delta)^{-1} \langle q_{\mathbf{T}}, \delta \cdot q_{\mathbf{T}} \rangle_{\text{disc}}$ is invariant under both the left and the right action of \mathbf{T} .

To see that the polynomials are actually equal, write $\mathbf{T} = g\mathbf{PA}g^{-1}$ with $g \in \mathbf{G}(\mathbb{C})$. Let $q_0(x, y) = xy$ be the discriminant 1 binary quadratic form of the torus \mathbf{PA} . We have $q_{\mathbf{T}}(x, y) = \pm g \cdot q_0(x, y)$. Without loss of generality the sign in the equality is positive.

We now reduce the claim to the case $\mathbf{T} = \mathbf{PA}$.

$$\begin{aligned} (\det \delta)^{-1} \langle q_{\mathbf{T}}, \delta \cdot q_{\mathbf{T}} \rangle_{\text{disc}} &= (\det g \delta g^{-1})^{-1} \langle q_0, (g^{-1} \delta g) \cdot q_0 \rangle_{\text{disc}} \\ \Psi_{+1}^{\mathbf{T}}(\delta) - \Psi_{-1}^{\mathbf{T}}(\delta) &= \Psi_{+1}(g^{-1} \delta g) - \Psi_{-1}(g^{-1} \delta g) \end{aligned}$$

For $\mathbf{T} = \mathbf{PA}$ the claims follows from a direct computation of both expressions. \square

Corollary 5.2. *The polynomials $\Psi_{+1}^{\mathbf{T}}$ and $\Psi_{-1}^{\mathbf{T}}$ are defined over \mathbb{Q} .*

Proof. As $q_{\mathbf{T}}$ is a quadratic form over \mathbb{Q} and $\langle \cdot, \cdot \rangle_{\text{disc}}$ is defined over \mathbb{Q} we deduce from the previous proposition that $\Psi_{+1}^{\mathbf{T}} - \Psi_{-1}^{\mathbf{T}}$ is defined over \mathbb{Q} .

The claim follows by the relation $\Psi_{+1}^{\mathbf{T}} + \Psi_{-1}^{\mathbf{T}} = 1$. \square

Remark 5.3. In higher rank we do not have an available linear representation having the same properties as the representation of \mathbf{PGL}_2 on \mathcal{Q} . The natural analogue is the action of \mathbf{PGL}_n on $\bigwedge^{n-1} \mathfrak{gl}_n$ which is fruitfully exploited in [ELMV09]. Yet this representation for $n > 2$ has plenty of lines whose stabilizer's identity component is not a maximal torus.

In what follows we have to study the canonical generators attached to rational tori without the aid of a linear representation. This is mainly done using the action of the Galois group of the splitting field on the generators and the algebraic relations between them.

We note that Bhargava [Bha04] has discovered a linear representation of a higher rank group such that the identity components of all the line stabilizers are tori, although not maximal ones. See also the generalization by Wood [Woo14].

6. DOUBLE TORUS QUOTIENT FOR CENTRAL SIMPLE ALGEBRAS

We are now in position to use the results of the previous parts to study packets in the projective group of units and in the group of units of norm 1 in a central simple algebra.

Let \mathbf{B} be a central simple algebra over \mathbb{F} considered as an \mathbb{F} -algebra object in the category of affine algebraic varieties. Denote the reduced norm by $\text{Nrd}: \mathbf{B} \rightarrow \mathbb{G}_m$. When restricted to the group of units, $\mathbf{GL}_1(\mathbf{B})$, it is an \mathbb{F} -character. Let \mathbf{G} be a reductive linear algebraic group equal either to $\mathbf{PGL}_1(\mathbf{B})$ or $\mathbf{SL}_1(\mathbf{B}) := \ker(\text{Nrd}|_{\mathbf{GL}_1(\mathbf{B})})$. The linear algebraic group \mathbf{G} is defined over \mathbb{F} and it is either an inner \mathbb{F} -form of \mathbf{SL}_n or of \mathbf{PGL}_n . All inner \mathbb{F} -forms of \mathbf{PGL}_n and of \mathbf{SL}_n arise this way. See [IS01, Chapter III, §1.4] for details.

The groups $\mathbf{PGL}_1(\mathbf{B})$ and $\mathbf{SL}_1(\mathbf{B})$ are isogenous. The simply connected form is $\mathbf{SL}_1(\mathbf{B})$ and the adjoint one is $\mathbf{PGL}_1(\mathbf{B})$.

Let $\mathbf{T} < \mathbf{G}$ a maximal torus defined over \mathbb{F} . There is a unique maximal commutative subalgebra $\mathbf{E} < \mathbf{B}$ defined over \mathbb{F} such that $\mathbf{T} = \mathbf{PGL}_1(\mathbf{E})$ or $\mathbf{T} = \mathbf{SL}_1(\mathbf{E})$ depending whether \mathbf{G} is the adjoint or simply connected form respectively. The ring $\mathbb{K} := \mathbf{E}(\mathbb{F})$ is an étale-algebra of degree n over \mathbb{F} . The torus \mathbf{T} is anisotropic over \mathbb{F} if and only if \mathbb{K} is a field.

6.1. Double Torus Quotient over a Splitting Field. We don't have an explicit description of the double torus quotient $\mathbf{T} \parallel^{\mathbf{G}} \mathbf{T}$ over \mathbb{F} , but as we will see in this section we can use our description of¹³ $\mathbf{SA} \parallel^{\mathbf{SL}_n} \mathbf{SA}$ to derive an explicit description of $\mathbf{T} \parallel^{\mathbf{G}} \mathbf{T}$ after extending the scalars to a splitting field of \mathbf{T} . In other words, the double torus quotient varieties for different rational tori \mathbf{T} are all \mathbb{F} -forms of the standard double torus quotient $\mathbf{SA} \parallel^{\mathbf{SL}_n} \mathbf{SA}$.

Denote by \mathbb{L}/\mathbb{F} the splitting field of \mathbf{T} , equivalently \mathbf{E} , i.e. the unique minimal field extension of \mathbb{F} over which \mathbf{T} , equivalently \mathbf{E} , splits¹⁴.

A splitting field for \mathbf{E} always splits the central simple algebra as well. That is there exists an \mathbb{L} -isomorphism of algebras $\phi: \mathbf{B}_{\mathbb{L}} \rightarrow \mathbf{M}_{n,\mathbb{L}}$ (see the discussion in [GS06, §2.2]). When restricted to $\mathbf{G}_{\mathbb{L}}$ this induces an isomorphism $\mathbf{G}_{\mathbb{L}} \rightarrow \mathbf{SL}_{n,\mathbb{L}}$ or $\mathbf{G}_{\mathbb{L}} \rightarrow \mathbf{PGL}_{n,\mathbb{L}}$ which we also denote by ϕ .

This isomorphism sends $\mathbf{E}_{\mathbb{L}}$ to a split maximal commutative subalgebra in $\mathbf{M}_{n,\mathbb{L}}$. Lets insure that this subalgebra is the standard diagonal one by replacing ϕ with the composition of ϕ with an inner automorphism sending $\phi(\mathbf{E}_{\mathbb{L}})$ to the standard diagonal subalgebra, which we denote by $\mathbf{Diag}_{\mathbb{L}}$. Equivalently, we replace ϕ with an inner automorphism sending the torus $\phi(\mathbf{T}_{\mathbb{L}})$ to the standard diagonal torus: $\mathbf{PA}_{\mathbb{L}}$ for the adjoint form and $\mathbf{SA}_{\mathbb{L}}$ for the simply connected one¹⁵.

The properties of the universal categorical quotient in Theorem 3.1 assures us that $(\mathbf{T} \parallel^{\mathbf{G}} \mathbf{T})_{\mathbb{L}} \cong \mathbf{T}_{\mathbb{L}} \parallel^{\mathbf{G}_{\mathbb{L}}} \mathbf{T}_{\mathbb{L}}$. Therefore, the map ϕ induces an isomorphism $(\mathbf{T} \parallel^{\mathbf{G}} \mathbf{T})_{\mathbb{L}} \cong (\mathbf{SA} \parallel^{\mathbf{SL}_n} \mathbf{SA})_{\mathbb{L}}$.

We can now transport using ϕ our explicit coordinates $\{\Psi_{\sigma}^0\}_{\sigma \in S_n}$ from $\mathbf{SA} \parallel^{\mathbf{SL}_n} \mathbf{SA}$ to $(\mathbf{T} \parallel^{\mathbf{G}} \mathbf{T})_{\mathbb{L}}$. We wish to rewrite the polynomials Ψ_{σ}^0 using intrinsic notions similar to §4.1.3. For this we bring the classical definition of a complete set of primitive orthogonal idempotents.

Definition 6.1. An element of a unital ring $e_0 \in R$ is called an *idempotent* if $e_0^2 = e_0$. The idempotent e_0 is *non-trivial* if $e_0 \neq 0, 1$ and it is *primitive* if it cannot be written a sum of two non-trivial idempotents.

¹³Recall that we have a natural isomorphism $\mathbf{SA} \parallel^{\mathbf{SL}_n} \mathbf{SA} \cong \mathbf{PA} \parallel^{\mathbf{PGL}_n} \mathbf{PA}$.

¹⁴We say that a commutative algebra of degree n over \mathbb{L} is split if it is isomorphic as an algebra to \mathbb{L}^n .

¹⁵One doesn't need to work with the standard diagonal subalgebra here, any maximal commutative subalgebra of $\mathbf{M}_{n,\mathbb{L}}$ defined and split over \mathbb{F} will do.

Two idempotents $e_1, e_2 \in R$ are *orthogonal* if $e_1 e_2 = e_2 e_1 = 0$. A set of idempotents $e_1, \dots, e_n \in R$ is called a *complete set of primitive orthogonal idempotents* if all the e_i 's are mutually orthogonal primitive idempotents and $1 = e_1 + \dots + e_n$.

If R is commutative then a complete set of primitive orthogonal idempotents is unique, up to permutation, if it exists.

Proposition 6.2.

- (1) For each $1 \leq i \leq n$ let e_i^0 be the diagonal matrix with all zero entries except for a single 1 entry in the (i, i) place.
A complete set of primitive orthogonal idempotents for $\mathbf{Diag}_{\mathbb{L}}(\mathbb{L})$ is given by $\{e_i^0\}_{i=1}^n$. The ϕ^{-1} image of this set is a complete set of primitive orthogonal idempotents in $\mathbf{E}_{\mathbb{L}}(\mathbb{L})$. Write $e_i = \phi^{-1}(e_i^0)$ for those primitive orthogonal idempotents.
- (2) Fix an order of e_1, \dots, e_n . We identify the absolute Weyl group with symmetric group on the ordered complete set of primitive orthogonal idempotents and with the standard symmetric group on $\{1, \dots, n\}$ in a consistent manner. For all $\sigma \in \mathbf{W}_{\mathbf{T}}(\mathbb{L})$ we have $e_{\sigma(i)} = \sigma.e_i$.
- (3) The pullback to $(\mathbf{T} \backslash \mathbf{G} // \mathbf{T})_{\mathbb{L}}$ of Ψ_{σ}^0 is

$$\Psi_{\sigma}(g) := (\Psi_{\sigma}^0 \circ \phi)(g) = \mathrm{Nrd} \left(\sum_{i=1}^n (\sigma.e_i) g e_i \right) \cdot \mathrm{Nrd}(g)^{-1}$$

We call the polynomials $\{\Psi_{\sigma}\}_{\sigma \in \mathbf{W}_{\mathbf{T}}(\mathbb{L})}$ the **canonical generators** of the ring of regular functions of $(\mathbf{T} \backslash \mathbf{G} // \mathbf{T})_{\mathbb{L}}$.

Proof. The first two parts of the proposition are straightforward. The third part follows immediately from the facts that the reduced norm is exactly the determinant map for the matrix algebra and that ϕ , being an isomorphism of central simple algebras, is reduced-norm preserving. \square

The idempotents $e_1, \dots, e_n \in E_{\mathbb{L}} := \mathbf{E}_{\mathbb{L}}(\mathbb{L})$ form a base for $E_{\mathbb{L}}$ as an \mathbb{L} -vector space. One can use other bases for $E_{\mathbb{L}}$ to express the canonical generators. To do this we will need the reduced trace form. The central simple algebra $\mathbf{B}_{\mathbb{L}}$ carries a natural non-degenerate bilinear form, which is the reduced trace form Trd . This forms restricts to a non-degenerate bilinear form on $E_{\mathbb{L}}$ which is just the standard trace form on the étale algebra.

Lemma 6.3. Let $b_1, \dots, b_n \in E_{\mathbb{L}}$ be a basis for $E_{\mathbb{L}} := \mathbf{E}_{\mathbb{L}}(\mathbb{L})$ as an \mathbb{L} -vector space. Let $\check{b}_1, \dots, \check{b}_n$ the dual basis with respect to the reduced trace, i.e. $\mathrm{Trd}(\check{b}_i b_j) = \delta_{i,j}$. For any σ in the absolute Weyl group we have

$$\Psi_{\sigma}(g) = \mathrm{Nrd} \left(\sum_{i=1}^n \sigma.\check{b}_i \cdot g \cdot b_i \right) \cdot \mathrm{Nrd}(g)^{-1}$$

Proof. For a linear endomorphism $\rho \in \mathrm{End}_{\mathbb{L}}(E_{\mathbb{L}})$ denote by ρ^{\dagger} the adjoint operator with respect to the reduced trace.

Notice that e_1, \dots, e_n is an orthonormal basis with respect to the reduced trace. Hence if $(\rho_{i,j})_{i,j=1}^n$ is the matrix associated to the endomorphism ρ with respect to the basis e_1, \dots, e_n , then the matrix associated with ρ^\dagger is just the transposed matrix $(\rho_{j,i})_{i,j=1}^n$.

Choose $\rho \in \text{End}_{\mathbb{L}}(E)$ such that $\rho(e_i) = b_i$ for all $i = 1, \dots, n$, then $\rho^\dagger(\check{b}_i) = e_i$. Write $b_i = \sum_{j=1}^n \rho_{i,j} e_j$. A calculation now gives

$$\begin{aligned} \sum_{i=1}^n \sigma \cdot \check{b}_i \cdot g \cdot b_i &= \sum_{i=1}^n \sigma \cdot \check{b}_i \cdot g \cdot \left(\sum_{j=1}^n \rho_{i,j} e_j \right) = \sum_{j=1}^n \sigma \cdot \left(\sum_{i=1}^n \rho_{i,j} \check{b}_i \right) \cdot g \cdot e_j \\ &= \sum_{j=1}^n \sigma \cdot \rho^\dagger(\check{b}_i) \cdot g \cdot e_j = \sum_{j=1}^n \sigma \cdot e_j \cdot g \cdot e_j \end{aligned}$$

This concludes the proof. \square

6.2. Galois Action. The splitting field \mathbb{L} is always a Galois extension of the base field \mathbb{F} . In this section we study the action of the Galois group $\mathfrak{G} := \text{Gal}(\mathbb{L}/\mathbb{F})$ on the map ϕ and derive from this the way the Galois group acts on the algebraic numbers $\Psi_\sigma(g)$ for $g \in \mathbf{G}(\mathbb{F})$.

Galois Descent. We briefly review basic facts from the theory of Galois descent for quasiprojective algebraic varieties in a form useful to us. As all our varieties are affine they are quasiprojective.

There is a natural action of $\mathfrak{G} := \text{Gal}(\mathbb{L}/\mathbb{F})$ on the variety $\mathbf{X}_{\mathbb{L}}$ by \mathbb{F} -automorphisms. By an abuse of notation we denote the automorphism of $\mathbf{X}_{\mathbb{L}}$ induced by $\sigma \in \mathfrak{G}$ also by σ .

Given two algebraic varieties \mathbf{X}, \mathbf{Y} defined over \mathbb{F} , we have an induced action of \mathfrak{G} on $\text{Mor}_{\mathbb{F}}(\mathbf{X}_{\mathbb{L}}, \mathbf{Y}_{\mathbb{L}})$ by $f^\sigma := \sigma \circ f \circ \sigma^{-1}$. If f is an isomorphism then so is f^σ for each $\sigma \in \mathfrak{G}$. This action extends to the arrow category in the following way. If we have the following morphisms of algebraic varieties over \mathbb{F}

$$\begin{array}{ccc} \mathbf{X}' & & \mathbf{Y}' \\ \downarrow & & \downarrow \\ \mathbf{X} & & \mathbf{Y} \end{array}$$

Together with additional horizontal morphisms making the following diagram commute

$$\begin{array}{ccc}
\mathbf{X}'_{\mathbb{L}} & \xrightarrow{f'} & \mathbf{Y}'_{\mathbb{L}} \\
\downarrow & & \downarrow \\
\mathbf{X}_{\mathbb{L}} & \xrightarrow{f} & \mathbf{Y}_{\mathbb{L}}
\end{array}$$

Then the following diagram commutes for each $\sigma \in \mathfrak{G}$

$$\begin{array}{ccc}
\mathbf{X}'_{\mathbb{L}} & \xrightarrow{f'^{\sigma}} & \mathbf{Y}'_{\mathbb{L}} \\
\downarrow & & \downarrow \\
\mathbf{X}_{\mathbb{L}} & \xrightarrow{f^{\sigma}} & \mathbf{Y}_{\mathbb{L}}
\end{array}$$

Set $\text{Aut}(\mathbf{Y}'_{\mathbb{L}} \rightarrow \mathbf{Y}_{\mathbb{L}})$ to be the group of pairs of automorphisms of $\mathbf{Y}'_{\mathbb{L}}$ and $\mathbf{Y}_{\mathbb{L}}$ which intertwine with the vertical morphism $\mathbf{Y}'_{\mathbb{L}} \rightarrow \mathbf{Y}_{\mathbb{L}}$. The map $\sigma \mapsto (f'^{\sigma} \circ f'^{-1}, f^{\sigma} \circ f^{-1})$ is 1-cocycle in $H^1(\mathfrak{G}, \text{Aut}(\mathbf{Y}'_{\mathbb{L}} \rightarrow \mathbf{Y}_{\mathbb{L}}))$.

Moreover if we denote $\mathfrak{G}_{f'} := \{\sigma \in \mathfrak{G} \mid f'^{\sigma} = f'\}$ and \mathbb{M}/\mathbb{F} is the field extension corresponding to the subgroup $\mathfrak{G}_{f'}$ then Galois descent for quasiprojective varieties provides the existence of the dotted morphism making the following diagram commute

$$\begin{array}{ccc}
\mathbf{X}'_{\mathbb{M}} & \overset{f'_{\mathbb{M}}}{\dashrightarrow} & \mathbf{Y}'_{\mathbb{M}} \\
\uparrow & & \uparrow \\
\mathbf{X}'_{\mathbb{L}} & \xrightarrow{f'} & \mathbf{Y}'_{\mathbb{L}}
\end{array}$$

In particular, if f' is an isomorphism then so is $f'_{\mathbb{M}}$.

Galois Descent for The Map ϕ . We are going to apply those generalities to the case $\mathbf{X} = \mathbf{B}$, $\mathbf{Y} = \mathbf{M}_n$, $\mathbf{X}' = \mathbf{PGL}_1(\mathbf{E})$, $\mathbf{Y}' = \mathbf{PA}$. The morphisms are ϕ and $\phi|_{\mathbf{PGL}_1(\mathbf{E})_{\mathbb{L}}}$, the restriction of ϕ to $\mathbf{PGL}_1(\mathbf{E})_{\mathbb{L}}$. The schematic image of $\phi|_{\mathbf{PGL}_1(\mathbf{E})_{\mathbb{L}}}$ is exactly $\mathbf{PA}_{\mathbb{L}}$.

The Skolem-Noether theorem implies that for each $\sigma \in \mathfrak{G}$ there exists $n_{\sigma} \in \mathbf{GL}_n(\mathbb{L})$ such that $\phi^{\sigma} = \text{Ad}_{n_{\sigma}} \circ \phi$ where $\text{Ad}_{n_{\sigma}}$ is the conjugation by n_{σ} . The equivalence class of n_{σ} in $\mathbf{PGL}_n(\mathbb{L})$ is uniquely determined by this equality. Lets denote this class by $[n_{\sigma}]$.

Because the Galois action is well defined in the arrow category

$$\left(\phi|_{\mathbf{PGL}_1(\mathbf{E})_{\mathbb{L}}} \right)^{\sigma} = \text{Ad}_{n_{\sigma}} \circ \phi|_{\mathbf{PGL}_1(\mathbf{E})_{\mathbb{L}}}$$

A fortiori, $\text{Ad}_{n_{\sigma}}(\mathbf{PA}_{\mathbb{L}}) = \mathbf{PA}_{\mathbb{L}}$, thus $[n_{\sigma}] \in N_{\mathbf{PGL}_n(\mathbf{PA})}(\mathbb{L})$.

We can now define a natural homomorphism of finite groups $\eta: \mathfrak{G} \rightarrow \mathbf{W}(\mathbb{L})$, where \mathbf{W} is the Weyl group of \mathbf{PA} . This homomorphism is defined

by the composition of the following maps

$$(12) \quad \mathfrak{G} \xrightarrow{\sigma \mapsto [n_\sigma]} N_{\mathbf{PGL}_n}(\mathbf{PA})(\mathbb{L}) \rightarrow N_{\mathbf{PGL}_n}(\mathbf{PA})/\mathbf{PA}(\mathbb{L}) = \mathbf{W}(\mathbb{L})$$

Because \mathbf{PA} is split over \mathbb{L} the group $\mathbf{W}(\mathbb{L})$ is equal to the absolute Weyl group of \mathbf{PA} .

Note that a priori, the map $\mathfrak{G} \rightarrow \mathbf{W}(\mathbb{L})$ is only a 1-cocycle, but as the torus \mathbf{PA} is already split over \mathbb{F} the action of \mathfrak{G} on $\mathbf{W}(\mathbb{L})$ is trivial, hence η is a homomorphism.

Moreover, we have a natural isomorphism between the Weyl group of \mathbf{PA} in \mathbf{PGL}_n and the Weyl group of \mathbf{SA} in \mathbf{SL}_n , we identify them both by abuse of notation. As ϕ and the Galois action on ϕ are defined at the central simple algebra level, all the discussion from hereon is applicable directly both to the adjoint form and to the simply connected one.

Proposition 6.4. *The homomorphism of finite groups $\eta: \mathfrak{G} \rightarrow \mathbf{W}(\mathbb{L})$ defined in (12) is injective.*

Proof. By abuse of notation we identify between elements of the Weyl group and the corresponding automorphisms of the torus. The discussion above implies that for all $\sigma \in \mathfrak{G}$ we have $\phi|_{\mathbf{PGL}_1(\mathbf{E})_{\mathbb{L}}}^\sigma = \eta(\sigma) \circ \phi|_{\mathbf{PGL}_1(\mathbf{E})_{\mathbb{L}}}$. Therefore, the Galois group stabilizer of $\phi|_{\mathbf{PGL}_1(\mathbf{E})_{\mathbb{L}}}$ is $\mathfrak{G}_{\phi|_{\mathbf{PGL}_1(\mathbf{E})_{\mathbb{L}}}} = \ker \eta$. Galois descent implies that the torus $\mathbf{PGL}_1(\mathbf{E})$ is split already over the subfield which corresponds to $\ker \eta$. Yet \mathbb{L} is the *minimal* splitting field of $\mathbf{PGL}_1(\mathbf{E})$, hence $\ker \eta$ is trivial. \square

6.2.1. Galois Action on Canonical Generators. We see that the Galois action on ϕ factors through the Weyl group. This allows us to compute the way in which the canonical generators of a rational point transform under the Galois group. By abuse of notation we denote both the \mathbb{L} -points in the Weyl group of \mathbf{PA} and the \mathbb{L} -points in the Weyl group of \mathbf{T} by W , those abstract groups are isomorphic through ϕ . In addition, because of the previous proposition we can treat \mathfrak{G} as a subgroup of W . Henceforth we avoid writing explicitly the homomorphism η .

We turn to describe the action of the Galois group on the canonical generators at a rational point.

Proposition 6.5. *Let $g \in \mathbf{G}(\mathbb{F})$ and $\tau \in \mathfrak{G}$, then for every $\sigma \in W$*

$$\tau \cdot \Psi_\sigma(g) = \Psi_{\tau\sigma\tau^{-1}}(g)$$

Proof. Let $n_\tau \in N_{\mathbf{PGL}_n}(\mathbf{PA})(\mathbb{L})$ be a representative of $\tau \in W$ such that $\phi^\tau = \text{Ad}_{n_\tau} \circ \phi$.

Recall that Ψ_σ is defined already over \mathbb{F} and that g is an \mathbb{F} -point, hence

$$\begin{aligned}
\tau.\Psi_\sigma(g) &= \tau.(\Psi_\sigma^0(\phi(g))) = \Psi_\sigma^0(\tau.(\phi(g))) = \Psi_\sigma^0(\phi^\tau(g)) \\
&= \Psi_\sigma^0(n_\tau\phi(g)n_\tau^{-1}) = \Psi_\sigma(n_\tau g n_\tau^{-1}) \\
&= \text{Nrd} \left(\sum_{i=1}^n (\sigma.e_i)\phi^{-1}(n_\tau)g\phi^{-1}(n_\tau)^{-1}e_i \right) \text{Nrd}(g)^{-1} \\
&= \text{Nrd} \left(\sum_{i=1}^n ((\sigma\tau^{-1}).e_i) g(\tau^{-1}.e_i) \right) \text{Nrd}(g)^{-1} \\
&= \text{Nrd} \left(\sum_{i=1}^n ((\tau\sigma\tau^{-1}).e_i) \cdot g \cdot e_i \right) \text{Nrd}(g)^{-1} = \Psi_{\tau\sigma\tau^{-1}}(g)
\end{aligned}$$

□

Unlike the case of \mathbf{PGL}_2 the canonical generators of rational points are not necessarily rational, except for¹⁶ Ψ_{id} . Nevertheless, we understand rather well their Galois orbits. Specifically, when $\mathfrak{G} \cong S_n$ each $\Psi_\sigma(g)$ belongs to the subfield of \mathbb{L} which corresponds to the centralizer subgroup $Z_{S_n}(\sigma)$ and the Galois orbits of the canonical generators correspond to conjugacy classes in S_n . Thus the number of those orbits is the partition number $p(n)$ which for large n is approximately $\frac{1}{4n\sqrt{3}} \exp\left(\pi\sqrt{\frac{2n}{3}}\right)$. Of course, we have in addition numerous algebraic relations between the generators. We now combine those algebraic relations with Proposition 6.5. This is a place where 2-transitivity of the Galois group is heavily used.

Corollary 6.6. *Assume that \mathfrak{G} is 2-transitive. Let $g \in \mathbf{G}(\mathbb{F})$ and let $\sigma \in W$ be a element of the Weyl group without fixed points. If $\Psi_\sigma(g) = 0$ then for every $\tau \neq \text{id}$ we have $\Psi_\tau(g) = 0$ and $\Psi_{\text{id}}(g) = 1$. Therefore the image of g in $\mathbf{T} \backslash \mathbf{G} // \mathbf{T}$ is $\mathbf{T}e\mathbf{T}$.*

Proof. For every $\tau \neq \text{id}$ we look at $\mathcal{C}_\tau = \{v\tau v^{-1} \mid v \in \mathfrak{G}\} \subset W \cong S_n$. The set \mathcal{C}_τ has a complete set of roots in the sense of Proposition 4.6, hence by the same proposition there exists $v \in \mathfrak{G}$ such that $\Psi_{v\tau v^{-1}}(g) = 0$. But $\Psi_\tau(g)$ is Galois conjugate to $\Psi_{v\tau v^{-1}}(g)$ so $\Psi_\tau(g) = 0$ as well.

To calculate $\Psi_{\text{id}}(g)$ we use the relation between the canonical generators coming from the Leibniz formula

$$\sum_{\tau \in W} \Psi_\tau(g) = 1$$

Because $\Psi_\tau(g) = 0$ for $\tau \neq \text{id}$ we have $\Psi_{\text{id}}(g) = 1$.

By now we have proved the $\Psi_\tau(g) = \Psi_\tau(e)$ for all $\tau \in W$. Because the Ψ_τ 's generate the whole ring of regular functions on $(\mathbf{T} \backslash \mathbf{G} // \mathbf{T})_{\mathbb{L}}$ the image of g as an \mathbb{L} -point in $(\mathbf{T} \backslash \mathbf{G} // \mathbf{T})_{\mathbb{L}}$ is equal to the image of e . Yet because

¹⁶This has been confirmed using the SageMath mathematical software [S⁺15].

the \mathbb{F} -points of a variety naturally *inject* into the \mathbb{L} -points, we conclude that the image of g in $\mathbf{T} \backslash \mathbf{G} // \mathbf{T}$ is already equal to the image of the identity. \square

7. PACKETS IN CENTRAL SIMPLE ALGEBRAS

We begin by describing the setup for S -arithmetic quotients coming from central simple algebras. In particular, we write down the discriminant data explicitly in terms of rings associated to maximal commutative subalgebras.

Our goal is to study the integrality properties of the canonical generators evaluated at a point associated to two torus orbits coming from the same packet.

The type of results we are about to prove are the simplest to state when $\mathbb{F} = \mathbb{Q}$. Then if $\delta_L \mathbf{T}(\mathbb{A})g_{\mathbb{A}}, \delta_R \mathbf{T}(\mathbb{A})g_{\mathbb{A}}$ with $\delta_R, \delta_L \in \mathbf{G}(\mathbb{Q})$ are two representatives of the same homogeneous toral set then $D_f \Psi_{\sigma}(g_L^{-1}g_R)$ is integral, where D_f is the product of the local archimedean discriminants of the homogeneous toral set. For a general number field \mathbb{F} we need to replace D_f by a suitable ideal of $\mathcal{O}_{\mathbb{F}}$.

These results are crucial, for they allows us to apply rudimentary geometry of numbers later on. This is akin to the simple fact that, in rank 1, the discriminant inner product of two binary *integral* quadratic forms associated with two periodic torus orbits is integral.

7.1. Setting. First of all we describe our setup. We keep the notations of the previous section.

Fix an $\mathcal{O}_{\mathbb{F}}$ order Ω in $\mathbf{B}(\mathbb{F})$. Recall that we denote by \mathbb{F}_u the completion of \mathbb{F} at the place $u \in \mathcal{V}_{\mathbb{F}}$. For u nonarchimedean let Ω_u be the closure of Ω in $\mathbf{B}(\mathbb{F}_u)$.

Fix a finite set of places of \mathbb{F} , denoted by S , such that the following holds

- (1) all the archimedean places are included in S ,
- (2) there is a place in S over which \mathbf{B} is isotropic¹⁷,
- (3) The set S is large enough so that

$$\mathbf{PGL}_1(\mathbf{B})(\mathbb{A}) = \mathbf{PGL}_1(\mathbf{B})(\mathbb{F}) \cdot \mathbf{PGL}_1(\mathbf{B})(\mathbb{F}_S) \cdot \prod_{u \notin S} \mathbf{PGL}_1(\Omega_u)$$

And the same for $\mathbf{SL}_1(\mathbf{B})$. That is these algebraic groups have class number 1 with respect to S and the integral structure induced by¹⁸ Ω .

Define $K_u < \mathbf{G}(\mathbb{F}_u)$ to be $\mathbf{PGL}_1(\Omega_u)$ or $\mathbf{SL}_1(\Omega_u)$ for the adjoint and the simply connected forms respectively. The group K_u is a compact open subgroup of $\mathbf{G}(\mathbb{F}_u)$.

Let $K_S = \prod_{u \notin S} K_u$ and define $\Gamma = K_S \cap \mathbf{G}(\mathbb{F})$ where the intersection is taken with respect to the *diagonal* embedding of $\mathbf{G}(\mathbb{F})$. Then Γ is a lattice

¹⁷This is required so that the S -arithmetic group of units of norm 1 is not compact.

¹⁸One can deduce results analogues to ours for smaller sets S not fulfilling this assumption by taking quotients. Otherwise one can deduce all our results directly avoiding this assumption with the downside of obfuscating many statements.

in the S -arithmetic product $G_S := \prod_{u \in S} \mathbf{G}(\mathbb{F}_u)$, again with respect to the diagonal embedding.

Using the fact that \mathbf{G} has class number one with respect to S , we can identify $\Gamma \backslash G_S$ with $\mathbf{G}(\mathbb{F}) \backslash \mathbf{G}(\mathbb{A}) / K_S$.

7.2. Homogeneous Toral Sets for Central Simple Algebras.

Homogeneous Toral Sets. Let $\mathbf{T} < \mathbf{G}$ be a fixed maximal torus defined and anisotropic over \mathbb{F} . Let $g_{\mathbb{A}} \in \mathbf{G}(\mathbb{A})$. Recall that an adelic homogeneous toral set is a subset of $\mathbf{G}(\mathbb{F}) \backslash \mathbf{G}(\mathbb{A})$ given by

$$Y = \mathbf{G}(\mathbb{F}) \backslash \mathbf{T}(\mathbb{A}) g_{\mathbb{A}}$$

Local Tori. A homogeneous toral set $\mathbf{G}(\mathbb{F}) \backslash \mathbf{T}(\mathbb{A}) g_{\mathbb{A}}$, $g_{\mathbb{A}} = (g_u)_{u \in \mathcal{V}_{\mathbb{F}}}$, defines for all $u \in \mathcal{V}_{\mathbb{F}}$ a torus over \mathbb{F}_u

$$\mathbf{H}_u := g_u^{-1} \mathbf{T}_{\mathbb{F}_u} g_u$$

The homogeneous toral set is a collection of periodic orbits for the geometric tori $\mathbf{H}_u(\mathbb{F}_u)$.

Denote by $\Psi_{\sigma}^{\mathbf{T}}$ the canonical generators $\mathbf{T} \backslash \mathbf{G} // \mathbf{T}$ over a splitting field and by $\Psi_{\sigma}^{\mathbf{H}_u}$ the canonical generators for $\mathbf{H}_u \backslash \mathbf{G}_{\mathbb{F}_u} // \mathbf{H}_u$ over a splitting field. The equality $\Psi_{\sigma}^{\mathbf{T}}(\lambda) = \Psi_{\sigma}^{\mathbf{H}_u}(g_u^{-1} \lambda g_u)$ holds in any field extension of \mathbb{F}_u splitting the torus \mathbf{T} .

7.3. Discriminant Data. For the cases we study $\mathbf{G} = \mathbf{PGL}_1(\mathbf{B})$ and $\mathbf{G} = \mathbf{SL}_1(\mathbf{B})$ we can provide a more concrete description of the discriminant data. It will be useful in studying the arithmetic properties of the canonical generators.

We now fix a homogeneous toral set $Y := \mathbf{G}(\mathbb{F}) \backslash \mathbf{T}(\mathbb{A}) g_{\mathbb{A}}$ with $g_{\mathbb{A}} = (g_u)_{u \in \mathcal{V}_{\mathbb{F}}}$

7.3.1. Local Nonarchimedean Discriminant. Fix $u \in \mathcal{V}_{\mathbb{F},f}$. Denote by $\mathbf{C}_u < \mathbf{B}_{\mathbb{F}_u}$ the maximal commutative subalgebra such that $\mathbf{PGL}_1(\mathbf{C}_u) = \mathbf{H}_u$ or $\mathbf{SL}_1(\mathbf{C}_u) = \mathbf{H}_u$ for the adjoint and the simply connected forms respectively. The commutative \mathbb{F}_u -algebra $C_u := \mathbf{C}_u(\mathbb{F}_u)$ is a degree n étale-algebra over \mathbb{F}_u .

Recall that Ω_u is the closure of Ω in $\mathbf{B}(\mathbb{F}_u)$. This is an order in $\mathbf{B}(\mathbb{F}_u)$. The local analogue of the global order is the ring¹⁹ $\mathcal{R}_u := C_u \cap \Omega_u$.

Definition 7.1. The *relative local discriminant* of \mathcal{R}_u is

$$\mathcal{D}_u := \det(\text{Trd}(f_i f_j))_{1 \leq i, j \leq n}$$

where f_1, \dots, f_n is an $\mathcal{O}_{\mathbb{F}_u}$ basis for \mathcal{R}_u . We could have chosen a different base for \mathcal{R}_u and get a different value for the relative local discriminant, but all those values would differ only by a square of a unit [Cas86, §7.6]. Hence

¹⁹This is not necessarily an integral domain unless C_u is a field.

the relative local discriminant is a well defined class in $\mathcal{O}_{\mathbb{F}_u}/\mathcal{O}_{\mathbb{F}_u}^\times{}^2$. We fix some representative for \mathcal{D}_u .

The local discriminant D_u of Y whose definition appears in §2.4.2 is almost equal to the *absolute* discriminant of \mathcal{R}_u , $|\mathcal{D}_u|_u^{-1}$ [ELMV11, Lemma 9.5]. The two notions differ by a constant factor which for almost all places u is equal to 1. *We take the liberty to ignore this non-consequential subtlety and redefine the local discriminant of a homogeneous toral set to be equal hereon to the absolute discriminant of \mathcal{R}_u , i.e. $D_u := |\mathcal{D}_u|_u^{-1}$.*

7.3.2. Local Archimedean Discriminant. Recall that in order to calculate the local discriminant at an archimedean place u we had a choice of a norm on $(\bigwedge^r \mathfrak{g}(\mathbb{F}_u))^{\otimes 2}$ with $r = n - 1$. We restrict ourselves to a norm of a specific type which will be comfortable later on.

Set $\overline{\mathbb{F}_u}$ to be the algebraic closure of \mathbb{F}_u , as $\overline{\mathbb{F}_u} \cong \mathbb{C}$ we identify them both an work over \mathbb{C} . A norm on $(\bigwedge^r \mathfrak{g}(\overline{\mathbb{F}_u}))^{\otimes 2}$ naturally restricts to a norm on $(\bigwedge^r \mathfrak{g}(\mathbb{F}_u))^{\otimes 2}$.

We have a decomposition of \mathbb{C} -vector spaces

$$\mathbf{B}(\mathbb{C}) = \mathbf{B}^0(\mathbb{C}) \oplus \text{Id } \mathbb{C}$$

Where $\mathbf{B}^0 := \ker \text{Trd}$ is the trace zero part of the algebra.

Let Q be an Hermitian inner product on $\mathbf{B}(\mathbb{C})$ such that the spaces $\mathbf{B}^0(\mathbb{C})$ and $\text{Id } \mathbb{C}$ are orthogonal to each other.

This in turn induces an inner product on $\mathfrak{g}(\mathbb{C})$ using the identification of $\mathfrak{g}(\mathbb{C})$ with the trace zero part $\mathbf{B}^0(\mathbb{C})$.

This inner product can be extended to an inner product on $\bigwedge^r \mathfrak{g}(\mathbb{C})$ using the standard determinant construction. This last inner product is a bilinear form on $\bigwedge^r \mathfrak{g}(\mathbb{C})$ so it extends to a linear functional on $(\bigwedge^r \mathfrak{g}(\mathbb{C}))^{\otimes 2}$. The absolute value of this linear functional will be the required norm.

In particular if we choose a base f_1, \dots, f_r for $\text{Ad}(g_u^{-1})\mathfrak{t}(\mathbb{F}_u)$ we can extend it to a base $f_0 = 1, f_1, \dots, f_n$ of $\mathbf{C}_u(\mathbb{F}_u)$ by identifying $\text{Ad}(g_u^{-1})\mathfrak{t}(\mathbb{F}_u)$ with the trace zero part of $\mathbf{C}_u(\mathbb{F}_u)$. For this base we can calculate the discriminant in the following way

$$(13) \quad D_u = \det(Q(f_i, f_j))_{1 \leq i, j \leq r} \cdot |\det(\text{Trd}(f_i f_j))_{1 \leq i, j \leq r}|^{-1}$$

$$(14) \quad = \det(Q(f_i, f_j))_{0 \leq i, j \leq r} \cdot |\det(\text{Trd}(f_i f_j))_{0 \leq i, j \leq r}|^{-1}$$

Expression (13) involves determinant of f_1, \dots, f_r and expression (14) involves determinant of f_0, f_1, \dots, f_r . The second expression is independent of the base we have chosen for $\mathbf{C}_u(\mathbb{C})$. Hence for Q of the form we are discussing, we can use (14) as the definition of the archimedean discriminant with any base we like for $\mathbf{C}_u(\mathbb{C})$.

7.3.3. Global Discriminant.

Matrix algebra over \mathbb{Q} . We start with describing the global discriminant in the classical setting of \mathbf{M}_n over $\mathbb{F} = \mathbb{Q}$.

The following description of the global discriminant from [ELMV09] and [ELMV11] is important for applications.

Let $\hat{u} \in S$ be a fixed place. Fix as well a split torus \mathbf{H}^0 over $\mathbb{Q}_{\hat{u}}$.

Lets consider only homogeneous toral sets for which $\mathbf{H}_{\hat{u}} = \mathbf{H}^0$ and $\mathbf{H}_u = \mathbf{T}_u$ for all $u \neq \hat{u}$. Notably, \mathbf{T} is assumed to be split over $\mathbb{Q}_{\hat{u}}$. We call such homogeneous toral sets *simple*.

Given \mathbf{T} there are no more then finitely many simple homogeneous toral sets corresponding to \mathbf{T} . They are parametrized by the absolute Weyl group of \mathbf{T} .

Notice that the general definition of the local discriminant is a property of the tori \mathbf{H}_u . In our concrete case all those tori either come from \mathbf{T} or are they are all equal to \mathbf{H}^0 at the place \hat{u} . Hence the local discriminant at the place \hat{u} does not depend on the simple homogeneous toral set. Its contribution to the global discriminant is immaterial.

On the other hand at all places $u \neq \hat{u}$ the local discriminant is a property of \mathbf{T} . Accordingly, the global discriminant of such a homogeneous toral set essentially depends only on \mathbf{T} .

As expected, the global discriminant in this case is actually an invariant of a global object. To such a homogeneous toral set one can attach a global order $\mathcal{R} := \mathbb{K} \cap \Omega$, where $\mathbb{K} = \mathbf{E}(\mathbb{Q})$ and \mathbf{E} is the maximal commutative subalgebra over \mathbf{T} . Recall that \mathbb{K} is a degree n field extension of \mathbb{Q} and \mathcal{R} is an order in this number field.

It is shown in [ELMV11, §6.3] that the discriminant of the order \mathcal{R} coincides up to a constant factor with the global discriminant of the homogeneous toral set. This equality of discriminants follows from the fact that the discriminant of an order can be calculated locally as well²⁰.

Relative nonarchimedean discriminant. We return to our general setting of a central simple algebra \mathbf{B} over a number field \mathbb{F} with Y a general homogeneous toral set.

We begin with the definition of the *absolute* nonarchimedean discriminant.

Definition 7.2. We define the *absolute nonarchimedean discriminant* of the homogeneous toral set to be $D_f = \prod_{u \in \mathcal{V}_f} D_u$ where the product is taken across all the nonarchimedean places.

There is a notion of a *relative* global nonarchimedean discriminant which will be useful to us. This notion refines the global discriminant of simple homogeneous toral sets for \mathbf{M}_n over \mathbb{Q} .

Definition 7.3. The *relative nonarchimedean discriminant* of the homogeneous toral set is the unique *ideal* \mathcal{D} of $\mathcal{O}_{\mathbb{F}}$ such that for any $u \in \mathcal{V}_{\mathbb{F},f}$ the closure of \mathcal{D} in $\mathcal{O}_{\mathbb{F}_u}$ is $\mathcal{D}_u \mathcal{O}_{\mathbb{F}_u}$.

²⁰The place \hat{u} splits in \mathbb{K} so the local discriminant of the order \mathcal{R} at \hat{u} is trivial.

One can see using the relation between the norm of an ideal and nonarchimedean valuations that

$$\mathrm{Nr}_{\mathbb{F}/\mathbb{Q}} \mathcal{D} = \prod_{u \in \mathcal{V}_{\mathbb{F},f}} |\mathcal{D}_u|_u^{-1} = \prod_{u \in \mathcal{V}_{\mathbb{F},f}} D_u = D_f$$

In particular, if $\mathbb{F}=\mathbb{Q}$ then $\mathcal{D} = D_f \mathbb{Z}$.

7.4. Denominators of Canonical Generators. Recall that we have fixed a homogeneous toral set $Y := \mathbf{G}(\mathbb{F}) \backslash \mathbf{T}(\mathbb{A})g_{\mathbb{A}}$.

Let $\delta_L \mathbf{T}(\mathbb{A})g_{\mathbb{A}}, \delta_R \mathbf{T}(\mathbb{A})g_{\mathbb{A}}$ with $\delta_L, \delta_R \in \mathbf{G}(\mathbb{F})$ be two representatives of the homogeneous toral set Y . We are interested what can be said about $\lambda := \delta_L^{-1} \delta_R$ when $\delta_R \mathbf{T}(\mathbb{A})g_{\mathbb{A}}$ belongs to a small neighborhood around $\delta_L \mathbf{T}(\mathbb{A})g_{\mathbb{A}}$. Specifically for each finite place u we are looking at pairs such that

$$\delta_R \mathbf{T}(\mathbb{F}_u)g_u \subset \delta_L \mathbf{T}(\mathbb{F}_u)g_u K_u$$

Or equivalently

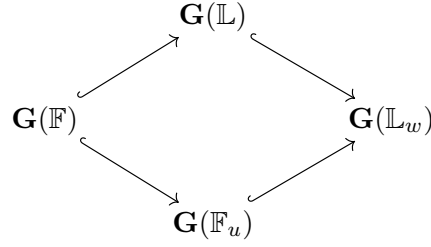
$$\begin{aligned} \lambda = \delta_L^{-1} \delta_R &\in \mathbf{G}(\mathbb{F}) \cap \prod_{u \in \mathcal{V}_{\mathbb{F},f}} \mathbf{T}(\mathbb{F}_u)g_u K_u g_u^{-1} \mathbf{T}(\mathbb{F}_u) \\ &= \mathbf{G}(\mathbb{F}) \cap \prod_{u \in \mathcal{V}_{\mathbb{F},f}} g_u \mathbf{H}_u(\mathbb{F}_u) K_u \mathbf{H}_u(\mathbb{F}_u) g_u^{-1} \end{aligned}$$

We would like to compute a denominator for $\Psi_{\sigma}^{\mathbf{T}}(\lambda) \in \mathbb{L}$ in each field extension \mathbb{L}_w , when w is a nonarchimedean place of \mathbb{L} . By a denominator we mean a w -adic integer $d_w \in \mathcal{O}_{\mathbb{L}_w}$ such that $d_w \Psi_{\sigma}^{\mathbf{T}}(\lambda) \in \mathcal{O}_{\mathbb{L}_w}$. Examining the rank 1 case one observes that a natural candidate for this denominator is the local discriminant of the torus. Actually, it will be the local *relative* discriminant.

Recall that as λ is an \mathbb{F} -point and the polynomials $\Psi_{\sigma}^{\mathbf{T}}$ for $\sigma \in W$ are defined over \mathbb{L} we have that $\Psi_{\sigma}^{\mathbf{T}}(\lambda) \in \mathbb{L}$. For a place w of \mathbb{L} extending u we fix a commutative diagram of embeddings

$$\begin{array}{ccc} & \mathbb{L} & \\ \swarrow & & \searrow \\ \mathbb{F} & & \mathbb{L}_w \\ \searrow & & \swarrow \\ & \mathbb{F}_u & \end{array}$$

This induces the following commutative diagram of natural injections for points in \mathbf{G}



We can write in $\mathbf{G}(\mathbb{F}_u)$: $g_u^{-1}\lambda g_u = h_u^L k_u h_u^R$ with $k_u \in K_u$ and $h_u^L, h_u^R \in \mathbf{H}_u(\mathbb{F}_u)$. These elementary facts imply that in \mathbb{L}_w one has

$$\Psi_\sigma^{\mathbf{T}}(\lambda) = \Psi_\sigma^{\mathbf{H}_u}(g_u^{-1}\lambda g_u) = \Psi_\sigma^{\mathbf{H}_u}(h_u^L k_u h_u^R) = \Psi_\sigma^{\mathbf{H}_u}(k_u)$$

The last equality holds because $\Psi_\sigma^{\mathbf{H}_u}$ is invariant under the left and right actions of \mathbf{H}_u . Hence for u nonarchimedean it is enough to consider expressions of the form $\Psi_\sigma^{\mathbf{H}_u}(k_u)$.

Proposition 7.4. *Let u be a nonarchimedean place of \mathbb{F} and let w be a place of \mathbb{L} above u . Assume that \mathbf{B} is unramified over u , equivalently \mathbf{G} is u -split. Assume that \mathcal{R}_u is the maximal order of $C_u := \mathbf{C}_u(\mathbb{F}_u)$. Then for all $\sigma \in W$ and for all $k_u \in K_u$ we have*

$$\mathcal{D}_u \Psi_\sigma^{\mathbf{H}_u}(k_u) \in \mathcal{O}_{\mathbb{L}_w}$$

Proof.

Sketch. We begin by providing a sketch of the proof. The idea is simple but the proof is cluttered with technical details.

- (1) Without loss of generality we can assume that Ω_u is a maximal order.
- (2) Over a nonarchimedean place u of \mathbb{F} where \mathbf{B} is unramified the central simple algebra $\mathbf{B}(\mathbb{F}_u)$ is isomorphic to a matrix algebra over \mathbb{F}_u .
- (3) The isomorphism from item 2 can be chosen so that the image of Ω_u is exactly the matrix ring over $\mathcal{O}_{\mathbb{F}_u}$.
- (4) The basic idea is to find a *nice* element $g \in \mathbf{GL}_n(\mathbb{L}_w)$ conjugating the standard diagonal commutative subalgebra of the matrix algebra to $C_w := \mathbf{C}_u(\mathbb{L}_w)$ and then transform $\Psi_\sigma^{\mathbf{H}_u}(k_u)$ to an expression involving primitive orthogonal idempotents over the standard diagonal torus, e_1^0, \dots, e_n^0 .
- (5) The expression for the canonical generator becomes

$$\Psi_\sigma^{\mathbf{H}_u}(k_u) = \text{Nrd} \left(\sum_{i=1}^n \sigma \cdot e_i^0 (g^{-1} k_u g) e_i^0 \right) \cdot \text{Nrd}(k_u^{-1})$$

- (6) Both e_i^0 and $\sigma \cdot e_i^0$ are in Ω_w which is the matrix ring over $\mathcal{O}_{\mathbb{L}_w}$. The same holds for $k_u \in K_u \subset \Omega_u \subset \Omega_w$.

- (7) *The heart of the argument:* We are able to choose g so that both g^{-1} and Δg are in the order Ω_w , where $\Delta^{-1} \in C_u$ generates the different ideal of \mathcal{R}_u which is principle. The norm of Δ contributes the \mathcal{D}_u factor to the end result.

The choice of a nice g as above is done in the following way

- (1) In matrix algebras the embedding of rational tori with a given \mathcal{R}_u are in bijection with homothety classes of bases for proper fractional ideals of \mathcal{R}_u .
- (2) If \mathcal{R}_u is maximal then it is a PID and all the embeddings correspond to bases of the trivial fractional ideal. This translates directly to the fact that we can choose g as above such that the rows of g^{-1} are a base for \mathcal{R}_u . In particular, g^{-1} is integral.
- (3) The rows of ${}^t g$, equivalently the columns of g , will be a dual base with respect to the reduced trace to the rows of g^{-1} ; hence they span the inverse different. To transform the matrix g into an integral one, we need to multiply it by the generator of the different ideal.

Structure of the Algebra over \mathbb{F}_u . The order Ω_u is contained in a maximal order $\Omega_u^{\max} \supseteq \Omega_u$. One has that K_u is a subset of $\mathbf{PGL}_1(\Omega_u^{\max})$ or $\mathbf{SL}_1(\Omega_u^{\max})$ for the adjoint and simply connected forms respectively.

The order \mathcal{R}_u is contained in the order $\Omega_u^{\max} \cap C_u$, where $C_u = \mathbf{C}_u(\mathbb{F}_u)$. As \mathcal{R}_u was assumed to be a maximal order this is actually an equality²¹. We see that the assumptions of the theorem would hold with Ω_u replaced by Ω_u^{\max} and that its conclusion for Ω_u follows from that for Ω_u^{\max} . We assume without loss of generality that $\Omega_u = \Omega_u^{\max}$.

As B_u is unramified it is isomorphic to the matrix algebra $\mathbf{M}_n(\mathbb{F}_u)$. Moreover, by [AG60, Theorem 3.5 and Theorem 3.8] we can choose the isomorphism $\iota : B_u \xrightarrow{\sim} \mathbf{M}_n(\mathbb{F}_u)$ so that $\iota(\Omega_u) = \mathbf{M}_n(\mathcal{O}_{\mathbb{F}_u})$ (see also [Rei75, Theorem 17.3]). By abuse of notation we will identify B_u with $\mathbf{M}_n(\mathbb{F}_u)$ and Ω_u with its image.

Let $B_w := B_u \otimes_{\mathbb{F}_u} \mathbb{L}_w \cong \mathbf{M}_n(\mathbb{L}_w)$ and let $\Omega_w := \mathbf{M}_n(\mathcal{O}_{\mathbb{L}_w})$. The ring Ω_w is a maximal order in B_w and $\Omega_w \cap B_u = \Omega_u$.

Let Diag_w be the diagonal commutative algebra in $\mathbf{M}_n(\mathbb{L}_w)$ and $A_w = \mathbf{PGL}_1(\text{Diag}_w)$ or $A_w = \mathbf{SL}_1(\text{Diag}_w)$ for the adjoint and simply connected forms respectively. Write $T_w := \mathbf{T}(\mathbb{L}_w)$. The tori T_w and A_w are both split, hence there exists $g_0 \in \mathbf{G}(\mathbb{L}_w)$ such that $T_w = g_0 A_w g_0^{-1}$. It follows that $C_w = g_0 \text{Diag}_w g_0^{-1}$, where $C_w := \mathbf{C}(\mathbb{L}_w)$. Any element of $g_0 N_{\mathbf{GL}_n(\mathbb{L}_w)}(\text{Diag}_w)$ will also conjugate those two commutative algebras to each other. Our aim now is to find a conjugating element whose matrix rows are a base for a proper fractional ideal \mathcal{I} of \mathcal{R}_u in a suitable sense.

Fractional Ideals. Lets explicate what we mean by a proper fractional ideal of \mathcal{R}_u . A full $\mathcal{O}_{\mathbb{F}_u}$ -lattice $\mathcal{J} \subseteq C_u$ is an \mathcal{R}_u fractional ideal if $\mathcal{R}_u \mathcal{J} \subseteq \mathcal{J}$.

²¹This is not the significant use of the maximality of \mathcal{R}_u .

The ring associated to a \mathcal{J} is

$$(15) \quad \mathcal{O}_{\mathcal{J}} := \{x \in C_u \mid x\mathcal{J} \subseteq \mathcal{J}\}$$

The fractional ideal is proper for \mathcal{R}_u if $\mathcal{O}_{\mathcal{J}} = \mathcal{R}_u$.

The étale-algebra C_u is a product of fields $C_u \cong \prod_{v \in \mathcal{W}_u} \mathbb{K}_u$ ²². The fields \mathbb{K}_v for $v \in \mathcal{W}_u$ ²³ are finite extensions of \mathbb{F}_u and $\sum_{v \in \mathcal{W}_u} [\mathbb{K}_v : \mathbb{F}_u] = n$.

Let $1_v \in C_u$ be the identity element of \mathbb{K}_v . Obviously $e = \sum_{v \in \mathcal{W}_u} 1_v$. By the maximality assumption for \mathcal{R}_u we have $\mathcal{R}_u \cong \prod_{v \in \mathcal{W}_u} \mathcal{O}_{\mathbb{K}_v}$. We can use this decomposition of \mathcal{R}_u to decompose any \mathcal{R}_u fractional ideal \mathcal{J} into a sum of $\mathcal{O}_{\mathbb{K}_v}$ fractional ideals $\mathcal{J} \cong \bigoplus_{v \in \mathcal{W}_u} \mathcal{J}_v$, where $\mathcal{J}_v := 1_v \mathcal{J}$. It holds that \mathcal{J} is \mathcal{R}_u -proper if and only if \mathcal{J}_v is $\mathcal{O}_{\mathbb{K}_v}$ proper for all $v \in \mathcal{W}_u$.

If \mathcal{J} is proper then each \mathcal{J}_v is a proper fractional ideal of the Discrete Valuation Ring $\mathcal{O}_{\mathbb{K}_v}$ ²⁴, hence it is principle and invertible. We conclude that \mathcal{J} itself is principle and invertible. One can choose $a_{\mathcal{J}} \in C_u^\times$ such that $\mathcal{J} = a_{\mathcal{J}} \mathcal{R}_u$.

For each fractional ideal \mathcal{J} one can define the dual fractional ideal

$$(16) \quad \widetilde{\mathcal{J}} = \{x \in C_u \mid \text{Trd}(x\mathcal{J}) \subseteq \mathcal{O}_{\mathbb{F}_u}\}$$

The dual is proper if \mathcal{J} is. In particular, the local inverse different $\widetilde{\mathcal{R}}_u$ is proper and principle²⁵. We write $\widetilde{\mathcal{R}}_u = \Delta^{-1} \mathcal{R}_u$ for $\Delta \in \mathcal{R}_u^\times$. Essentially by definition, Δ can be chosen so that $\text{Nrd}(\Delta) = \mathcal{D}_u$.

The Associated Fractional Idea. We grossly imitate the proof of [ELMV09, Corollary 4.4] to show that a conjugating element can be chosen so its rows are in a suitable manner a base for a proper fractional ideal.

We start by constructing an \mathbb{F}_u -vector space isomorphism $j: C_u \rightarrow \mathbb{F}_u^n$. For each $v \in \mathcal{W}_u$ we have a linear endomorphism of \mathbb{F}_u^n given by $a \mapsto 1_v \cdot a$, where the right hand side is the multiplication of a matrix by a vector. Because $1_v \neq 0$ for each v , the kernel of this endomorphism is a proper linear subspace of \mathbb{F}_u^n . The union of a finite collection of proper subspaces never exhausts a vector space over characteristic 0, hence there exists $a \in \mathbb{F}_u^n$ such that $1_v \cdot a \neq 0$ for all $v \in \mathcal{W}_u$. Let $j(x) := x \cdot a$. Notice that j intertwines the action of C_u on itself by matrix-matrix multiplication with the action of C_u on \mathbb{F}_u^n by matrix-vector multiplication.

To see that j is an isomorphism we prove it has a trivial kernel. For each $0 \neq x \in C_u$ one has $x = \sum_{v \in \mathcal{W}_u} x 1_v$ and $x 1_v$ can be identified with the \mathbb{K}_v component of x . In particular, there exists v_0 , depending on x , such that

²²When \mathbf{H}_u is an extension of scalars of an anisotropic \mathbb{F} torus then $\mathbb{K} := \mathbf{C}(\mathbb{F})$ is a field. Weak approximation for number fields implies $C_u \cong \prod_{v|u} \mathbb{K}_v$ where v runs over the places of \mathbb{K} over u . In the general case one cannot identify \mathcal{W}_u with a set of places of some fixed field.

²³We can consider \mathcal{W}_u as a set of equivalence classes of valuation on finite field extensions of \mathbb{F}_u .

²⁴This is one of the significant uses of the maximality assumption.

²⁵Second significant use of the maximality assumption.

$x1_{v_0} \neq 0$. Let $y_{v_0} \in C_u$ be the inverse of $x1_{v_0}$ in \mathbb{K}_{v_0} , then $y_{v_0}x = 1_{v_0}$. If $0 \neq x \in \ker j$ then $x \cdot a = 0$ and $0 = y_{v_0}x \cdot a = 1_{v_0} \cdot a$ which is a contradiction.

The fractional ideal we seek is the $\mathcal{O}_{\mathbb{F}_u}$ -lattice $\mathcal{I} := j^{-1}(\mathcal{O}_{\mathbb{F}_u}^n)$. Denote the canonical base elements for \mathbb{F}_u^n by $b_i = (0, \dots, 0, 1, 0, \dots, 0)$ with 1 in the i place for $1 \leq i \leq n$. Let $\beta_i := j^{-1}(b_i)$; this is a base of \mathcal{I} . Notice that for any $x = (x_{i,j})_{1 \leq i,j \leq n} \in C_u \subset \mathbf{M}_n(\mathbb{F}_u)$ we have

$$x\beta_j = j^{-1}(xb_j) = \sum_{i=1}^n x_{i,j}j^{-1}(b_i) = \sum_{i=1}^n x_{i,j}\beta_i$$

This implies immediately that $\mathcal{O}_{\mathcal{I}} = \mathbf{M}_n(\mathcal{O}_{\mathbb{F}_u}) \cap C_u = \mathcal{R}_u$, i.e. \mathcal{I} is a proper \mathcal{R}_u fractional ideal.

The Conjugating Matrix. Fix e_1, \dots, e_n – an ordered complete set of primitive orthogonal idempotents of C_w . We embed \mathcal{I} back into C_w by defining an \mathbb{L}_w -algebra isomorphism $\iota: C_w \rightarrow \mathbb{L}_w^n$, given by

$$\iota(x) := (\text{Trd}(xe_1), \text{Trd}(xe_2), \dots, \text{Trd}(xe_n))$$

For every $x = (x_{i,j})_{1 \leq i,j \leq n} \in C_w$ we can write

$$\iota(x)\iota(\beta_j) = \iota(x\beta_j) = \sum_{i=1}^n x_{i,j}\iota(\beta_i)$$

Let $M_{\iota(x)} \in \mathbf{GL}_n(\mathbb{F}_u)$ be the *diagonal* matrix in the canonical basis corresponding to the linear transformation $a \mapsto \iota(x)a$. The equality above implies for any $x \in C_w$ that $g_{\mathcal{I}}M_{\iota(x)}g_{\mathcal{I}}^{-1} = x$, where $g_{\mathcal{I}} \in \mathbf{GL}_n(\mathbb{L}_w)$ is the base change matrix defined by $g_{\mathcal{I}}\iota(\beta_i) = b_i$. We conclude that $g_{\mathcal{I}}\text{Diag}_w g_{\mathcal{I}}^{-1} = C_w$.

The ideal \mathcal{I} is principle and invertible because it is proper. Write $\mathcal{I} = a\mathcal{R}_u$ for some $a \in C_u^\times$. The elements $a\beta_1, \dots, a\beta_n$ form a basis for $\mathcal{R}_u \cong \prod_{v \in \mathcal{W}_u} \mathcal{O}_{\mathbb{K}_v}$, hence they are all integral. As ι is an algebra isomorphism, we deduce that $r_i := \iota(a\beta_i)$ is integral for all i , viz. $r_i \in \mathcal{O}_{\mathbb{L}_w}^n$.

Lets define $g = g_{\mathcal{I}}M_{\iota(a^{-1})}$; then $g\text{Diag}_w g^{-1} = C_w$ and $g^{-1}b_i = \iota(a\beta_i) = r_i \in \mathcal{O}_{\mathbb{L}_w}^n$. We deduce that $g^{-1} \in \Omega_w$.

Integrality of Δg . We have shown that g^{-1} is integral, the last critical step will be to show the Δg is also in $\mathbf{M}_n(\mathcal{O}_{\mathbb{L}_w})$.

Because of the way we constructed the isomorphism ι , the reduced trace form on C_w is pushed forward by ι to the regular euclidean form on \mathbb{L}_w^n . In particular ${}^t g$ is the adjoint of g with respect to this bilinear form. Hence if $\check{r}_1, \dots, \check{r}_n$ is the dual base of r_1, \dots, r_n , then ${}^t g b_i = \check{r}_i$.

Notice that $\iota^{-1}(\check{r}_1), \dots, \iota^{-1}(\check{r}_n)$ is the dual base of $a\beta_1, \dots, a\beta_n$. Thus it is an $\mathcal{O}_{\mathbb{F}_u}$ base of $\widehat{\mathcal{R}_u} = \Delta^{-1}\mathcal{R}_u$. In particular, $\iota(\Delta)\check{r}_i \in \mathcal{O}_{\mathbb{L}_w}^n$ for all i . We see that $M_{\iota(\Delta)}{}^t g \in \mathbf{M}_n(\mathcal{O}_{\mathbb{L}_w})$, so by applying the transpose we have $\mathcal{O}_{\mathbb{L}_w} \ni gM_{\iota(\Delta)} = g(g^{-1}\Delta g) = \Delta g$.

Concluding the Proof. Let $e_1^0 = g^{-1}e_1g, \dots, e_n^0 = g^{-1}e_ng$. This is a complete set of primitive idempotents for Diag_w . We can always choose a representative for k_u in $\mathbf{GL}_1(\Omega_u)$ which we now use. Next we compute

$$\begin{aligned} \Psi_\sigma(k_u)D_u &= \text{Nrd}\left(\sum_{i=1}^n \sigma.e_i k_u e_i\right) \text{Nrd}(k_u^{-1}) \text{Nrd}(\Delta) \\ &= \text{Nrd}\left(\sum_{i=1}^n \sigma.e_i^0 (g^{-1}k_u g) e_i^0\right) \text{Nrd}(k_u^{-1}) \text{Nrd}(g^{-1}\Delta g) \\ &= \text{Nrd}\left(\sum_{i=1}^n \sigma.e_i^0 (g^{-1}k_u \Delta g) e_i^0\right) \text{Nrd}(k_u^{-1}) \end{aligned}$$

In the last line we have used the fact that $g^{-1}\Delta g \in \text{Delta}_w$.

Because $\sum_{i=1}^n \sigma.e_i^0 (g^{-1}k_u \Delta g) e_i^0$ is in the order Ω_w it has integral reduced norm. In addition, $k_u^{-1} \in \mathbf{GL}_1(\Omega_u)$ and it also has an integral reduced norm. This concludes the proof. \square

Unfortunately, the proof above works only if \mathbf{B} is unramified over u . Although it would be plausible that the conclusion of the proof holds under weaker assumptions, as is the case in rank 1, we can only produce the following result. This result for the ramified places is significantly weaker but it needs only to be applied for finitely many places of \mathbb{F} .

Proposition 7.5. *Let u be a nonarchimedean place of \mathbf{F} and let w be a place of \mathbb{L} above u . Assume that \mathcal{R} is the maximal order of \mathbb{K} . Then for all $\sigma \in W$ and for all $k_u \in K_u$ we have*

$$\mathcal{D}_u^{1+n/2} \Psi_\sigma(k_u) \in \mathcal{O}_{\mathbb{L}_w}$$

Proof. We carry notations from the poof of the previous theorem. Let r_1, \dots, r_n be an $\mathcal{O}_{\mathbb{F}_u}$ -base for \mathcal{R}_u , We shall call it the *integral* base. The dual base with respect to the reduced trace, $\check{r}_1, \dots, \check{r}_n$, is an $\mathcal{O}_{\mathbb{F}_u}$ -base to $\check{\mathcal{R}}_u = \Delta^{-1}\mathcal{R}_u$. In particular for all i we have $\Delta\check{r}_i \in \mathcal{R}_u$.

Using lemma 6.3 we can write

$$\begin{aligned} \Psi_\sigma(k_u) &= \text{Nrd}\left(\sum_{i=1}^n \sigma.r_i k_u \check{r}_i\right) \text{Nrd}(k_u^{-1}) \\ &= \text{Nrd}\left(\sum_{i=1}^n \sigma.r_i k_u (\Delta\check{r}_i)\right) \text{Nrd}(k_u^{-1}) \mathcal{D}_u^{-1} \end{aligned}$$

We would like to transform $\sum_{i=1}^n \sigma.r_i k_u (\Delta\check{r}_i)$ to an element of Ω_w . Both k_u and $\Delta\check{r}_i$ for all i are in Ω_u , but $\sigma.r_i$ is not necessarily so.

For each $1 \leq j \leq n$ we would like to write down in C_w the element $\sigma.r_j$ in the integral base r_1, \dots, r_n . To do this we need to find out the matrix

corresponding to the linear transformation defined by the Weyl element σ in the r_1, \dots, r_n base.

In C_w we have another natural base. This is the base of the orthongonal primitive idempotents e_1, \dots, e_n . We shall call this the *orthogonal* base. Let M be the matrix in the orthogonal base of the transformation sending e_i to r_i . Because all the r_i are integral we have $M \in \mathbf{M}_n(\mathcal{O}_{\mathbb{L}_w})$. By definition of the discriminant, we have $\det M = \sqrt{\mathcal{D}_u}$.

The matrix corresponding to σ in the orthogonal base is just the standard permutation matrix P_σ . Hence the matrix corresponding to σ in the *integral* base is $Q_\sigma := MP_\sigma M^{-1} = MP_\sigma M^{\text{adj}} \cdot (\det M)^{-1}$. Where $M^{\text{adj}} \in \mathbf{M}_n(\mathcal{O}_{\mathbb{L}_w})$ is the adjugate matrix of M , which is constructed from the minors of M .

We see that $\sqrt{\mathcal{D}_u} Q_\sigma = MP_\sigma M^{\text{adj}}$ is an integral matrix. This implies that for all j we have

$$\sqrt{\mathcal{D}_u} \sigma.r_j \in \text{Span}_{\mathcal{O}_{\mathbb{L}_w}}(r_1, \dots, r_n) = \Omega_w \cap C_w \subset \Omega_w$$

We have thus proved that $\sum_{i=1}^n \sqrt{\mathcal{D}_u} \sigma.r_i k_u(\Delta \check{r}_i) \in \Omega_w$. This concludes the proof if we notice that the determinant of the matrix $\text{diag}(\sqrt{\mathcal{D}_u}, \dots, \sqrt{\mathcal{D}_u})$ is exactly $\mathcal{D}_u^{n/2}$. \square

7.4.1. Archimedean Denominators. We will also need an archimedean analogue of Proposition 7.4. The proof boils down to the following trivial linear algebra lemma.

Lemma 7.6. *Let V be an n -dimensional vector space over \mathbb{C} endowed with an inner product $Q: V \times V \rightarrow \mathbb{C}$.*

Let $\epsilon_1, \dots, \epsilon_n$ be a base of V . We form the Gram matrix of $\epsilon_1, \dots, \epsilon_n \in V$ with respect to the inner product Q

$$\text{Gr} := (Q(\epsilon_i, \epsilon_j))_{1 \leq i, j \leq n}$$

Then there exists $U \in \mathbf{U}_n(\mathbb{C})$ and a diagonal matrix S such that

$$(17) \quad \text{Gr} = US^2U^{-1}$$

Evidently, $\det \text{Gr} = (\det S)^2$.

Moreover, the base $\{US^{-1}\epsilon_i\}_{1 \leq i \leq n}$ is an orthonormal base with respect to Q .

Proof. The matrix Gr is Hermitian, hence there exists a unitary diagonalization $\text{Gr} = UDU^{-1}$. The existence of a square root of \mathcal{D} follows from the non-degeneracy of Q . \square

Proposition 7.7. *Let u be an archimedean place of \mathbb{F} and let w be a place of \mathbb{L} above u . Denote by $|\cdot|_w$ the canonical absolute value on \mathbb{L} associated to w .*

Let $B_u \subset \mathbf{G}(\mathbb{F}_u)$ be a pre-compact set. Then for any $g \in B_u$ and for all $\sigma \in W$

$$|\Psi_\sigma^{\mathbf{H}_u}(g)|_w \ll_{B_u} D_u$$

Proof. We have that either $\mathbb{L}_w \cong \mathbb{F}_u$ or $\mathbb{L}_w \cong \overline{\mathbb{F}_u}$, where $\overline{\mathbb{F}_u} \cong \mathbb{C}$ is the algebraic closure of \mathbb{F}_u . In any case we can identify $\overline{\mathbb{L}_w} \cong \overline{\mathbb{F}_u} \cong \mathbb{C}$ where all the absolute values are compatible. Notice that the embedding of B_u in $\mathbf{G}(\mathbb{C})$ is pre-compact as well. We work over \mathbb{C} .

In order to define the archimedean discriminant we had to fix an inner product Q_u on $\mathbf{G}(\mathbb{F}_u)$. We assume that this inner product is the restriction of an Hermitian inner product Q on $\mathbf{G}(\mathbb{C})$ chosen as in 7.3.2.

Let $C := \mathbf{C}_u(\mathbb{C})$ be the maximal commutative subalgebra corresponding to \mathbf{H}_u and let e_1, \dots, e_n a complete set of primitive orthogonal idempotents on in C .

For any $g \in \mathbf{G}(\mathbb{C})$ we can write

$$\Psi_\sigma^{\mathbf{H}_u}(g) = \text{Nrd} \left(\sum_{i=1}^n e_{\sigma(i)} \cdot \text{Ad}(g)e_i \right)$$

We define a utility function $\psi: \mathbf{G}(\mathbb{C}) \times \mathbf{B}(\mathbb{C})^{n^2} \times \mathbf{B}(\mathbb{C})^{n^2} \rightarrow \mathbb{C}$

$$\psi(g, b_{i,j}^L, b_{i,j}^R)_{1 \leq i,j \leq n} := \text{Nrd} \left(\sum_{i,j=1}^n b_{i,j}^L \cdot \text{Ad}(g)b_{i,j}^R \right)$$

This is a continuous function so it is bounded on pre-compact sets. Let $K_{\mathbb{C}} \subset \mathbf{B}(\mathbb{C})$ be the norm 1 ball with respect to ²⁶ Q . Our goal is to show $D_u^{-1} \Psi_\sigma^{\mathbf{H}_u}(g) \in \psi(B_u \times (K_{\mathbb{C}})^{n^2} \times (K_{\mathbb{C}})^{n^2})$ which will prove the claim.

To calculate D_u we can use any base f_1, \dots, f_n of C and apply equation (14)

$$D_u = \det(Q(f_i, f_j))_{1 \leq i,j \leq n} \cdot \left| \det(\text{Trd}(f_i f_j))_{1 \leq i,j \leq n} \right|_w^{-1}$$

We can compute the discriminant using the complete set of primitive orthogonal idempotents e_1, \dots, e_n .

$$D_u = \det(Q(e_i, e_j))_{1 \leq i,j \leq n}$$

This is just the determinant of the Gram matrix Gr of e_1, \dots, e_n .

By Lemma 7.6 we can write $\text{Gr} = US^2U^{-1}$ with U Hermitian and S diagonal with $(\det S)^2 = D_u$. In addition, the Q -orthonormal vectors $f_i := US^{-1}e_i$, $1 \leq i \leq n$, all belong to $K_{\mathbb{C}}$.

Write $S^{-1} = \text{diag}(s_1, \dots, s_n)$ and let $\varsigma := \sum_{i=1}^n s_i e_i \in C_u$. We have

$$\begin{aligned} D_u^{-1} \Psi_\sigma^{\mathbf{H}_u}(g) &= \text{Nrd}(\sigma.\varsigma) \text{Nrd} \left(\sum_{i=1}^n e_{\sigma(i)} \cdot \text{Ad}(g)e_i \right) \text{Nrd}(\text{Ad}(g)\varsigma) \\ &= \text{Nrd} \left(\sum_{i=1}^n s_{\sigma(i)} e_{\sigma(i)} \cdot \text{Ad}(g)s_i e_i \right) \end{aligned}$$

□

²⁶This is a decent analogue for some purposes of the compact subgroup of the nonarchimedean case, hence the notation.

Notice that $s_i e_i = U^{-1} f_i$, hence each of the vectors $s_i e_i$ can be expressed as a linear combination of f_1, \dots, f_n with coefficients equal to the entries of U^{-1} . As U^{-1} is unitarian, all its coefficients are smaller then 1 in absolute value. This concludes the proof.

8. LOWER BOUND FOR ASYMPTOTIC ENTROPY

We continue with the notations of the previous sections.

8.1. Limit Entropy of Well Separated Orbits. We begin by defining the Bowen ball.

Definition 8.1. Let $a \in G_S$ be a semisimple element. Let $B \subset G_S$ be an identity neighborhood. For any $s < t \in \mathbb{Z}$ Define

$$B^{(s,t)} := a^{-s} B a^s \cap a^{-t} B a^t$$

If $B = \prod_{u \in S} B_u$ is a box then the $u \in S$ component of $B^{(s,t)}$ is $B_u^{(s,t)} := a_u^{-s} B_u a_u^s \cap a_u^{-t} B_u a_u^t$.

We call $B^{(s,t)}$ a *Bowen ball* and for $x \in \Gamma \backslash G_S$ we call $x B^{(s,t)}$ a *Bowen Ball around x* .

For a semisimple element $a \in G_S$ and $B \subset G_S$ chosen small enough we can use the Lie algebra of G_S to conceptually understand the behavior of the set $B^{(-t,t)}$ for large $t > 0$. The Lie algebra of G_S decomposes into eigenspaces of $\text{Ad}(a)$. All the eigenspaces on which $\text{Ad}(a)$ acts with an eigenvalue which is not of unit absolute value will be either contracted or expanded under the adjoint action of a . In particular, the preimage of $B^{(-t,t)}$ in the Lie algebra will contract in all the these eigenspaces. Hence for large t the set $B^{(-t,t)}$ will be a thin tube.

The reason we care about Bowen balls is that an exponential bound on the average measure of Bowen balls implies an entropy bound for a probability limit measure. The following proposition is an S -arithmetic analogue of [ELMV09, Proposition 3.2]. Its proof is the same as of the original proposition.

Proposition 8.2. *Fix a semisimple element $a \in G_S$. Suppose that $\{\mu_i\}_{i=1}^\infty$ is a sequence of a -invariant probability measures on $\Gamma \backslash G_S$ converging to a probability measure μ in the weak-* topology.*

Assume that for some fixed $\eta > 0$ we have a sequence of integers $\tau_i \rightarrow_{i \rightarrow \infty} \infty$ such that for any compact subset $F \subset \Gamma \backslash G_S$ there exists an identity neighborhood $B \subset G_S$ such that

$$\begin{aligned} & \mu_i \times \mu_i \left\{ (x, y) \in F \times F \mid y \in x B^{(-\tau_i, \tau_i)} \right\} \\ &= \int_F \mu_i \left(x B^{(-\tau_i, \tau_i)} \cap F \right) d\mu_i(x) \ll_F \exp(-2\eta\tau_i) \end{aligned}$$

Then the metric entropy of the a -action with respect to the measure μ satisfies $h_\mu(a) \geq \eta$.

8.2. Double Torus Quotient of a Bowen Ball. In this section we study canonical generators of points in a Bowen ball. We will show that the canonical generators are bounded in terms of the size of the Bowen ball.

Fix a place $\hat{u} \in S$ and denote $\hat{\mathbb{F}} := \mathbb{F}_{\hat{u}}$. Let $\mathbf{H} < \mathbf{G}_{\hat{\mathbb{F}}}$ be a maximal torus defined over $\hat{\mathbb{F}}$. Let $\hat{\mathbb{L}}/\hat{\mathbb{F}}$ be the splitting field of \mathbf{H} and denote by \hat{w} the unique place of $\hat{\mathbb{L}}$ with canonical absolute value $|\cdot|_{\hat{w}}$. For $f \in \hat{\mathbb{F}}$ we have $|f|_{\hat{w}} = |f|_{\hat{u}}^d$ for some fixed $d \in \mathbb{N}$. Evidently, \mathbf{B} is split over $\hat{\mathbb{L}}$.

We fix $a \in \mathbf{H}(\hat{\mathbb{F}})$, all the Bowen balls we discuss are with respect to this fixed a .

Denote by $\Psi_{\sigma}^{\mathbf{H}}$ the canonical generators of $(\mathbf{H} \backslash \mathbf{G}_{\hat{\mathbb{F}}} // \mathbf{H})_{\hat{\mathbb{L}}}$. Notice that \mathbf{H} is split over $\hat{\mathbb{L}}$ so the generators are defined over $\hat{\mathbb{L}}$. Our task is to bound $\Psi_{\sigma}^{\mathbf{H}}(g)$ when $g \in B_{\hat{u}}^{(s,t)}$.

There exists a maximal commutative subalgebra $\mathbf{C} < \mathbf{B}$ such that $\mathbf{H} = \mathbf{PGL}_1(\mathbf{C})$ or $\mathbf{H} = \mathbf{SL}_1(\mathbf{C})$ for the adjoint and simply connected forms respectively. Let $e_1^{\mathbf{H}}, \dots, e_n^{\mathbf{H}}$ a complete set of primitive orthogonal idempotents for the split commutative algebra $\mathbf{C}(\hat{\mathbb{L}})$. As usual we identify the absolute Weyl group of \mathbf{H} with the symmetric group on $e_1^{\mathbf{H}}, \dots, e_n^{\mathbf{H}}$.

Definition 8.3 (Coordinates relative to \mathbf{H}). As the algebra \mathbf{B} is split over $\hat{\mathbb{L}}$ there exists an isomorphism over $\hat{\mathbb{L}}$

$$(18) \quad \xi: \mathbf{B}_{\hat{\mathbb{L}}} \rightarrow \mathbf{M}_{n, \hat{\mathbb{L}}}$$

such that $\xi(\mathbf{C}_{\hat{\mathbb{L}}}) = \mathbf{Diag}_{\hat{\mathbb{L}}}$. Choose ξ so it is compatible with the fixed orderings of the primitive orthogonal idempotents in $\mathbf{C}_{\hat{\mathbb{L}}}(\hat{\mathbb{L}})$ and $\mathbf{Diag}_{\hat{\mathbb{L}}}(\hat{\mathbb{L}})$.

Recall that $x_{i,j}$ are the usual coordinate functions on the matrix algebra. We define

$$x_{i,j}^{\mathbf{H}} = x_{i,j} \circ \xi$$

The functions $x_{i,j}^{\mathbf{H}}$ are regular functions generating $\hat{\mathbb{L}}[\mathbf{B}_{\hat{\mathbb{L}}}]$. In particular, they are continuous with respect to the Hausdorff topology on $\mathbf{B}_{\hat{\mathbb{L}}}(\hat{\mathbb{L}})$.

Lemma 8.4. *Let σ be an element of the absolute Weyl group of \mathbf{H} . When considered as a function of $\mathbf{G}_{\hat{\mathbb{F}}}$, the canonical generator $\Psi_{\sigma}^{\mathbf{H}}$ can be written as*

$$\Psi_{\sigma}^{\mathbf{H}} = \text{sign } \sigma (\det)^{-1} \prod_{i=1}^n x_{\sigma(i), i}^{\mathbf{H}}$$

Proof. Notice that this is well defined both for the adjoint form and for the simply connected one. The claim follows directly from Propositions 4.1 and 6.2. \square

We need to explicate the relation between roots of \mathbf{H} and the set of roots R_{σ} associated to $\sigma \in W_{\mathbf{H}}$. The group $W_{\mathbf{H}}$ is the absolute Weyl group of \mathbf{H} which is identified with the symmetric group over the primitive orthogonal idempotents. Lets recall the definition of the set of roots of $\sigma \in W_{\mathbf{H}} \cong S_n$

$$R_{\sigma} := \{(\sigma(i), i) \mid 1 \leq i \leq n, \sigma(i) \neq i\}$$

The roots of \mathbf{H} are the non-trivial weights of the adjoint action of \mathbf{H} on the Lie algebra $\text{Lie}(\mathbf{G})$. Both for the adjoint and the simply connected forms the roots²⁷ $\alpha_{i,j} : \mathbf{H}_{\widehat{\mathbb{L}}} \rightarrow \mathbb{G}_m$ are indexed by pairs $\{(i, j) \mid 1 \leq i, j \leq n, i \neq j\}$. They can be defined for both forms by

$$\alpha_{i,j} := x_{i,i}^{\mathbf{H}} / x_{j,j}^{\mathbf{H}}$$

Hereafter when discussing elements of R_σ we identify the pair of integers $(\sigma(i), i) \in R_\sigma$ with the root $\alpha_{\sigma(i), i}$.

Proposition 8.5. *Let $|\cdot|_{\widehat{w}}$ be the standard absolute value associated to \widehat{w} on $\widehat{\mathbb{L}}$. Fix $\sigma \in W_{\mathbf{H}}$. Let R_σ be the set of roots associated to σ as in Proposition 4.6. Assume $B_{\widehat{u}} \subseteq \mathbf{G}(\widehat{\mathbb{F}})$ is pre-compact. The following holds for any $g \in B_{\widehat{u}}^{(s,t)}$*

$$|\Psi_\sigma^{\mathbf{H}}(g)|_{\widehat{w}} \ll_{\mathbf{H}, B_{\widehat{u}}} \prod_{\alpha \in R_\sigma} \min(|\alpha(a^s)|_{\widehat{w}}, |\alpha(a^t)|_{\widehat{w}})$$

Proof. Our starting point is Lemma 8.4. We raise the expression for $\Psi_\sigma^{\mathbf{H}}$ to the n 'th power

$$(\Psi_\sigma^{\mathbf{H}})^n = \text{sign } \sigma \prod_{i=1}^n \frac{(x_{\sigma(i), i}^{\mathbf{H}})^n}{\det}$$

We claim that for each $1 \leq i, j \leq n$ the function

$$\widetilde{x_{i,j}^{\mathbf{H}}} := (x_{\sigma(i), i}^{\mathbf{H}})^n \cdot (\det)^{-1}$$

is a regular function on $\mathbf{G}_{\widehat{\mathbb{L}}}$. Using the isomorphism ξ defined in (18) we can reduce this claim to the analogous claim for \mathbf{SL}_n and \mathbf{PGL}_n .

For the simply connected form $\mathbf{G}_{\widehat{\mathbb{L}}} \cong \mathbf{SL}_{n, \widehat{\mathbb{L}}}$ we treat the function $(\det)^{-1}$ as the constant function 1 and the claim is trivial.

For the adjoint case $\mathbf{G}_{\widehat{\mathbb{L}}} \cong \mathbf{PGL}_{n, \widehat{\mathbb{L}}}$ we look closer at the coordinate rings. The ring of regular function on $\mathbf{GL}_{n, \widehat{\mathbb{L}}}$ is $\widehat{\mathbb{L}}[\mathbf{GL}_n] = \widehat{\mathbb{L}}[x_{i,j}, (\det)^{-1}]_{1 \leq i, j \leq n}$ and the regular functions on $\mathbf{PGL}_{n, \widehat{\mathbb{L}}}$ are the elements of degree zero in $\widehat{\mathbb{L}}[\mathbf{GL}_n]$, where the degree is defined the same as for regular polynomials except that the degree of $(\det)^{-1}$ is $-n$. Our functions $\widetilde{x_{i,j}^{\mathbf{H}}}$ are degree zero, hence they are regular.

From the definition of $\alpha_{i,j}$ and $x_{i,j}^{\mathbf{H}}$ we see that for any $h \in H$

$$x_{i,j}^{\mathbf{H}} \circ \text{Ad}(h) = \alpha_{i,j}(h) \cdot x_{i,j}^{\mathbf{H}}$$

We tentatively define $\alpha_{i,i}$ to be the trivial character for all $1 \leq i \leq n$, i.e. $x_{i,i}^{\mathbf{H}}$ is invariant under conjugation by h .

For the normalized n 'th power functions

$$\widetilde{x_{i,j}^{\mathbf{H}}} \circ \text{Ad}(h) = \alpha_{i,j}(h)^n \cdot \widetilde{x_{i,j}^{\mathbf{H}}}$$

²⁷ \mathbf{H} splits over $\widehat{\mathbb{L}}$, so the roots can be defined over $\widehat{\mathbb{L}}$.

The set $B_{\widehat{u}}$ is pre-compact when embedded in $\mathbf{G}(\widehat{\mathbb{L}})$ because the topologies on $\mathbf{G}(\widehat{\mathbb{L}})$ and $\mathbf{G}(\widehat{\mathbb{F}})$ are compatible.

As the functions $\widehat{x_{i,j}^{\mathbf{H}}}$ are regular ones they are continuous with respect to the Hausdorff topology on $\mathbf{G}(\widehat{\mathbb{L}})$, in particular $|\widehat{x_{i,j}^{\mathbf{H}}}|_{\widehat{u}}$ is bounded on the pre-compact set $B_{\widehat{u}}$. Therefore for $g \in \text{Ad}(h)(B_{\widehat{u}})$

$$|\widehat{x_{i,j}^{\mathbf{H}}}(g)|_{\widehat{w}} \leq |\alpha_{i,j}(h)|_{\widehat{w}}^n \cdot \sup_{g \in B_{\widehat{u}}} |\widehat{x_{i,j}^{\mathbf{H}}}(g)|_{\widehat{w}}$$

We conclude that for $g \in B_{\widehat{u}}^{(s,t)}$ the following estimate holds

$$(19) \quad |\widehat{x_{i,j}^{\mathbf{H}}}(g)|_{\widehat{w}} \ll_{\mathbf{H}, B_{\widehat{u}}} \min(|\alpha_{i,j}(a^s)|_{\widehat{w}}^n, |\alpha_{i,j}(a^t)|_{\widehat{w}}^n)$$

Notice that for $i = j$ the character $\alpha_{i,i}$ is trivial and the bound does not depend on s and t .

The proposition follows from multiplying estimate (19) for all $(\sigma(i), i)$, $1 \leq i \leq n$, and taking the positive n 'th root. \square

8.3. Small Bowen Balls.

Split Place. We now fix once and for all a place $\widehat{u} \in S$ and denote $\widehat{\mathbb{F}} := \mathbb{F}_{\widehat{u}}$. Let $\mathbf{H} < \mathbf{G}_{\widehat{\mathbb{F}}}$ be an isotropic maximal torus defined over $\widehat{\mathbb{F}}$, i.e. $\text{rank}_{\widehat{\mathbb{F}}} \mathbf{H} > 0$.

Let $H := \mathbf{H}(\widehat{\mathbb{F}})$. We consider H as embedded in G_S in the natural way. The isotropy assumption is necessary for H to have non-trivial dynamics on $\Gamma \backslash G_S$.

Definition 8.6. A homogeneous toral set $\mathbf{G}(\widehat{\mathbb{F}}) \backslash \mathbf{T}(\widehat{\mathbb{A}})g_{\widehat{u}}$, $g_{\widehat{u}} = (g_u)_{u \in \mathcal{V}_{\widehat{\mathbb{F}}}}$, such that $\mathbf{H}_{\widehat{u}} := g_{\widehat{u}}^{-1} T_{\widehat{\mathbb{F}}} g_{\widehat{u}} = \mathbf{H}$ is called an *H invariant* homogeneous toral set.

The projection of Y to $\Gamma \backslash G_S$ is called an *H invariant* packet.

We split the proof of the entropy lower bound to two parts. The new result obtained from the methods presented here is essentially Theorem 8.9. The entropy lower bound presented in Theorem 1.2 follows from Theorem 8.9 using well known methods going back essentially to Linnik [Lin68]. In their modern form they have been developed in [ELMV09], [ELMV12], [EMV13].

8.3.1. Small Bowen Balls are Trivial. For $a \in H$ and an a -invariant probability measure μ on $\Gamma \backslash G_S$ we denote by $h_{\mu}(a)$ the Kolmogorov-Sinai entropy of the measure μ with respect to the \mathbb{Z} action by a . Let m be the Haar measure on $\Gamma \backslash G_S$, then

$$h_{\text{Haar}}(a) := h_m(a) = \frac{1}{2} |\log |\det \text{Ad}_a|_{\widehat{u}}| = \frac{1}{2d} \sum_{1 \leq i \neq j \leq n} |\log |\alpha_{i,j}(a)|_{\widehat{u}}|$$

Where the absolute value on the outside each $\log |\alpha_{i,j}(a)|_{\widehat{u}}$ is the regular absolute value on \mathbb{R} and $|f|_{\widehat{u}} = |f|_{\widehat{u}}^d$ for each $f \in \widehat{\mathbb{F}}$.

Definition 8.7. Let $Y = \mathbf{G}(\mathbb{F}) \backslash \mathbf{T}(\mathbb{A})g_{\mathbb{A}}$ be a homogeneous toral with local discriminants $(D_u)_{u \in \mathcal{V}_{\mathbb{F}}}$. Let \mathcal{V}_{ram} be the set of *finite* \mathbb{F} -places where \mathbf{B} is ramified. We define the ramified discriminant to be

$$D_{\text{ram}} := \prod_{u \in \mathcal{V}_{\text{ram}}} D_u$$

Definition 8.8. Let $Y = \mathbf{G}(\mathbb{F}) \backslash \mathbf{T}(\mathbb{A})g_{\mathbb{A}}$ be a homogeneous toral. For any finite place u of \mathbb{F} denote by $\mathbf{C}_u < \mathbf{B}_{\mathbb{F}_u}$ be the commutative algebra corresponding to the local torus $\mathbf{H}_u = g_u^{-1} \mathbf{T}g_u$. We say the Y is a homogeneous toral set of *maximal type* if for any finite u the order $\mathcal{R}_u := \Omega_u \cap C_u(\mathbb{F}_u)$ is maximal in the étale algebra $\mathbf{C}_u(\mathbb{F}_u)$.

Theorem 8.9. Let $Y = \mathbf{G}(\mathbb{F}) \backslash \mathbf{T}(\mathbb{A})g_{\mathbb{A}}$ be an H invariant homogeneous toral set of maximal type with discriminant D and ramified local discriminant D_{ram} . Let \mathbb{L} be the splitting field of \mathbf{T} . Assume $\mathfrak{G} := \text{Gal}(\mathbb{L}/\mathbb{F})$ is 2-transitive.

Let $a \in H$ and fix $B = \prod_{u \in S} B_u$ such that for all $\hat{u} \neq u \in S$ nonarchimedean the set B_u is contained in K_u .

There exists a constant κ depending only on B , \mathbb{F} and \mathbf{H} such that if

$$(20) \quad 2 \frac{h_{\text{Haar}}(a)}{n-1} \tau > \log \left(D D_{\text{ram}}^{n/2} \right) + \kappa$$

Then any $\lambda \in \mathbf{G}(\mathbb{F}) \cap \mathbf{T}(\mathbb{A})g_{\mathbb{A}} \left(B_u^{(-\tau, \tau)} \times K_S \right) g_{\mathbb{A}}^{-1} \mathbf{T}(\mathbb{A})$ belongs to $\mathbf{T}(\mathbb{F})$.

Proof. For now let κ be a free variable. Let λ be as in the theorem's conditions. Denote by W be the absolute Weyl group of \mathbf{T} .

Galois orbits. Recall that by Proposition 6.4 we can consider \mathfrak{G} as a subgroup of W .

Fix $\sigma \in W$. By Proposition 6.5 the Galois orbit of $\Psi_{\sigma}^{\mathbf{T}}(\lambda) \in \mathcal{O}_{\mathbb{L}}$ is

$$\{ \Psi_{\tau\sigma\tau^{-1}}^{\mathbf{T}}(\lambda) \mid \tau \in \mathfrak{G} \}$$

Denote $\mathcal{C} := \{ \tau\sigma\tau^{-1} \mid \tau \in \mathfrak{G} \}$ and let $|\mathcal{C}|$ be the cardinality of \mathcal{C} . We now define

$$\Psi_{\mathcal{C}}(\lambda) := \prod_{\omega \in \mathcal{C}} \Psi_{\omega}^{\mathbf{T}}(\lambda) \in \mathbb{F}$$

Archimedean bound for $\Psi_{\mathcal{C}}(\lambda)$. For each archimedean place $u \neq \hat{u}$ of \mathbb{F} let m be the number of places $w|u$ of $^{\text{28}} \mathbb{L}$. Applying Proposition 7.7 and using that $B_u^{(-\tau, \tau)} = B_u$ for all archimedean $u \neq \hat{u}$ we have

$$|\psi_{\mathcal{C}}(\lambda)|_u^m = \prod_{w|u} |\psi_{\mathcal{C}}(\lambda)|_w \leq (\kappa_0 D_u)^{|\mathcal{C}|m}$$

The constant $\kappa_0 > 0$ depends on B only. Set $\kappa_1 := \max(\kappa_0, 1)$.

²⁸We treat each pair of conjugate complex places as genuinely different.

Taking the positive real root of order m we have the necessary bound

$$(21) \quad |\psi_{\mathcal{C}}(\lambda)|_u \leq \kappa_1^{|\mathcal{C}|} D_u^{|\mathcal{C}|}$$

Nonarchimedean bound for $\Psi_{\mathcal{C}}(\lambda)$. For all nonarchimedean $u \neq \hat{u}$ we have²⁹

$$\lambda \in \mathbf{T}(\mathbb{F}_u) g_u K_u g_u^{-1} \mathbf{T}(\mathbb{F}_u)$$

For each nonarchimedean place $u \neq \hat{u}$ of \mathbb{F} where \mathbf{B} is ramified we apply Proposition 7.4

$$\begin{aligned} |\psi_{\mathcal{C}}(\lambda)|_u^{[\mathbb{L}:\mathbb{F}]} &= |\mathrm{Nr}_{\mathbb{L}/\mathbb{F}} \psi_{\mathcal{C}}(\lambda)|_u = \prod_{w|u} |\psi_{\mathcal{C}}(\lambda)|_w \\ &\leq \prod_{w|u} |\mathcal{D}_u|_w^{-|\mathcal{C}|} = |\mathrm{Nr}_{\mathbb{L}/\mathbb{F}} \mathcal{D}_u|_u^{-|\mathcal{C}|} = D_u^{|\mathcal{C}|[\mathbb{L}:\mathbb{F}]} \end{aligned}$$

If \mathbf{B} is ramified at $u \neq \hat{u}$ we apply the weaker Proposition 7.5 and have similarly

$$|\psi_{\mathcal{C}}(\lambda)|_u^{[\mathbb{L}:\mathbb{F}]} \leq D_u^{(1+n/2)|\mathcal{C}|[\mathbb{L}:\mathbb{F}]}$$

Taking the positive real root of order $[\mathbb{L}:\mathbb{F}]$ we have the necessary bounds

$$(22) \quad |\psi_{\mathcal{C}}(\lambda)|_u \leq D_u^{|\mathcal{C}|} \text{ If } \mathbf{B} \text{ is unramified at } u$$

$$(23) \quad |\psi_{\mathcal{C}}(\lambda)|_u \leq D_u^{(1+n/2)|\mathcal{C}|} \text{ Otherwise}$$

Exponential bound. It will be now important to choose σ that has *no fixed points*. We are going to calculate the exponential bound on $|\Psi_{\mathcal{C}}(\lambda)|_{\hat{u}}$.

Let $\widehat{\mathbb{L}}/\widehat{\mathbb{F}}$ be the splitting field of \mathbf{H} and denote by \hat{w} place of $\widehat{\mathbb{L}}$. Using Proposition 8.5 we deduce that

$$(24) \quad |\Psi_{\mathcal{C}}(\lambda)|_{\hat{w}} \leq \kappa_2^{|\mathcal{C}|} \exp \left(-\tau \sum_{\omega \in \mathcal{C}} \sum_{\alpha \in R_{\omega}} |\log |\alpha(a)|_{\hat{w}}| \right)$$

Where $k_2 > 0$ depends only on B . Notice that the outer absolute value of $|\log |\alpha(a)|_{\hat{w}}|$ is the usual absolute value on \mathbb{R} .

As $\Psi_{\mathcal{C}}(\lambda)$ belongs to \mathbb{F} it can be considered as an element of $\widehat{\mathbb{F}}$. Inequality (24) implies

$$|\Psi_{\mathcal{C}}(\lambda)|_{\hat{u}} \leq \kappa_2^{|\mathcal{C}|} \exp \left(-\frac{\tau}{d} \sum_{\omega \in \mathcal{C}} \sum_{\alpha \in R_{\omega}} |\log |\alpha(a)|_{\hat{w}}| \right)$$

How many times each root of \mathbf{H} appears in the sum above? Because \mathfrak{G} is 2-transitive it is easy to see that all the roots appear in the sum with the same multiplicity. There are totally $n(n-1)$ roots. Each $\omega \in \mathcal{C}$ contributes the same number of roots to the sum as σ , which contributes exactly n of them at it has *no fixed points*. Hence each root appears in the sum with multiplicity

$$\frac{n|\mathcal{C}|}{n(n-1)} = \frac{|\mathcal{C}|}{n-1}$$

²⁹If $u \in S$ then $B_u \subseteq K_u$.

In the expression for $2h_{\text{Haar}}(a)$ each root appears with multiplicity 1. We conclude that

$$(25) \quad |\Psi_{\mathcal{C}}(\lambda)|_{\hat{u}} \leq \kappa_2^{|\mathcal{C}|} \exp\left(-2 \frac{h_{\text{Haar}}(a)}{n-1} |\mathcal{C}| \tau\right)$$

Triviality of $\Psi_{\mathcal{C}}(\lambda)$. For each place of $u \neq \hat{u}$ we apply either bound (21) or (22) or (23) appropriately. For the place $u = \hat{u}$ we apply the exponential bound (25). Combining these we have

$$\begin{aligned} \text{Nr}_{\mathbb{A}} \Psi_{\mathcal{C}}(\lambda) &:= \prod_{u \in \mathcal{V}_{\mathbb{F}}} |\Psi_{\mathcal{C}}(\lambda)|_u \\ &\leq \left(\kappa_1^{[\mathbb{F}:\mathbb{Q}]} \kappa_2\right)^{|\mathcal{C}|} D_{\hat{u}}^{-|\mathcal{C}|} D^{|\mathcal{C}|} D_{\text{ram}}^{n/2|\mathcal{C}|} \exp\left(-2 \frac{h_{\text{Haar}}(a)}{n-1} |\mathcal{C}| \tau\right) \end{aligned}$$

The local discriminant $D_{\hat{u}}$ depends only on \mathbf{H} . Define $\kappa_3 = \kappa_1^{[\mathbb{F}:\mathbb{Q}]} \kappa_2 D_{\hat{u}}^{-1}$, it depends only on B , \mathbb{F} and \mathbf{H} .

We see that if

$$\begin{aligned} \kappa_3^{|\mathcal{C}|} D^{|\mathcal{C}|} D_{\text{ram}}^{n/2|\mathcal{C}|} \exp\left(-2 \frac{h_{\text{Haar}}(a)}{n-1} |\mathcal{C}| \tau\right) &< 1 \\ \iff 2 \frac{h_{\text{Haar}}(a)}{n-1} \tau &> \log\left(D D_{\text{ram}}^{n/2}\right) + \log \kappa_3 \end{aligned}$$

Then $\text{Nr}_{\mathbb{A}} \Psi_{\mathcal{C}}(\lambda) < 1$. But $\Psi_{\mathcal{C}}(\lambda) \in \mathbb{F}$ and from the product formula for the number field \mathbb{F} we deduce that $\Psi_{\mathcal{C}}(\lambda) = 0$.

Finishing the proof. We are now ready to set $\kappa = \log \kappa_3$. We have shown that if inequality (20) holds then $\Psi_{\mathcal{C}}(\lambda) = 0$. This in turn implies that there exists $\tau \in \mathfrak{G}$ such that $\Psi_{\tau\sigma\tau^{-1}}^{\mathbf{T}}(\lambda) = 0$.

By Corollary 6.6 the projection of $\lambda \in \mathbf{G}(\mathbb{F})$ to $\mathbf{T} \backslash \mathbf{G} // \mathbf{T}$ is $\mathbf{T}e\mathbf{T}$. Now we can use Proposition 3.6 to conclude that there exists $t \in \mathbf{T}(\mathbb{F})$ such that $\lambda = t$ and the claim is proved. \square

8.4. Proof of the Entropy Lower Bound. We are now ready to prove our lower bound on the asymptotic entropy. The reader should remember that our final argument is an extension of a rank 1 argument which is weaker than Linnik's full powered method. Indeed, in rank 1 Linnik's results are akin to an optimal bound on the entropy [Lin68], [ELMV12]. A generalization of Linnik's basic lemma and a finer analysis of integral points on the variety $\mathbf{T} \backslash \mathbf{G} // \mathbf{T}$ in conjugation with the Galois action remain open.

In addition we have no contribution to the question of escape of mass in the non-cocompact case. We assume a priori that mass does not escape. This is unnecessary if \mathbf{B} is a division algebra as \mathbf{G} is compact in that case.

Statement of Theorem (1.2). *Suppose we have a sequence of H invariant homogeneous toral sets of maximal type $Y_i = \mathbf{G}(\mathbb{F}) \backslash \mathbf{T}_i(\mathbb{A})^{g_i}$ with \mathbf{T}_i a torus defined and anisotropic over \mathbb{F} and $g_i \in G_{\mathbb{A}}$. Let \mathbb{L}_i/\mathbb{F} be the splitting field of \mathbf{T}_i . We assume for all i that $\text{Gal}(\mathbb{L}_i/\mathbb{F})$ is 2-transitive.*

Denote by D_i the global discriminant of Y_i . Assume $D_i \rightarrow_{i \rightarrow \infty} \infty$. Let $D_{\text{ram},i}$ be the ramified discriminant of Y_i which is the product of local discriminant at finite places where \mathbf{B} is ramified. Suppose $D_{\text{ram},i} = D_i^{o(1)}$

Let μ_i be the probability measure on $\Gamma \backslash G^S$ induced by the probability measure on the homogeneous toral set Y_i . If μ_i converges in the weak-* topology to a probability measure μ on $\Gamma \backslash G^S$ then for any $a \in H$ we have³⁰

$$h_\mu(a) \geq \frac{h_{\text{Haar}}(a)}{2(n-1)}$$

Remark 8.10. The volume of the packet is known to be equal to $D_i^{1/2+o(1)}$, see [ELMV11, Theorem 4.8]. Although the proof in [ELMV11] is written for the case $\mathbf{B} = \mathbf{M}_n$ it applies verbatim to any central simple algebra \mathbf{B} . Notice that any torus in \mathbf{B} over a local field can be embedded in \mathbf{M}_n with the same local order³¹ \mathcal{R}_u . The computation of the volume depends only on this data if the norms are chosen consistently.

Proof of Theorem 1.2. The theorem would follow from combining Theorem 8.9 with Proposition 8.2 ([ELMV09, Proposition 3.2]).

The necessary bound on Bowen balls. We define

$$\eta = \frac{h_{\text{Haar}}(a)}{n-1}$$

Choose B as in Theorem 8.9 and such that $B_u^{(-\tau, \tau)} \subseteq B_u$ for all³² $\tau \geq 0$. Proposition 8.2 implies that the theorem would follow if for each $\varepsilon > 0$ we can find a sequence of positive integers $\tau_i \rightarrow_{i \rightarrow \infty} \infty$ such that for any compact $F \subset \Gamma \backslash G^S$

$$(26) \quad \int_F \mu_i \left(x B^{(-\tau_i, \tau_i)} \right) d\mu_i(x) \ll_{F, \mathbb{F}, B, \mathbf{H}, \varepsilon} \exp(-(\eta - \varepsilon)\tau_i)$$

Let $Z_i \subset \Gamma \backslash G^S$ be the projection of Y_i . By choosing τ_i appropriately, we are going to show that inequality (26) holds individually for any Bowen ball $x B^{(-\tau_i, \tau_i)}$ with $x \in Z_i$. This will imply the theorem.

Volume of a small Bowen ball. Theorem 8.9 suggests that we choose

$$(27) \quad \tau_i = \frac{\log \left(D_i D_{\text{ram},i}^{n/2} \right)}{2\eta} + \kappa + 1 = \frac{\log(D_i) (1 + o(1))}{2\eta} + \kappa + 1$$

Fix $x \in Z_i$ and let $q = \delta_0 t_0 g_i k_0 \in G(\mathbb{F}) \mathbf{T}_i(\mathbb{A}) g_i K_S$ be an adelic representative of x . We can now bound the measure of the Bowen ball around x corresponding to τ_i . Recall that the measure μ_i is the projection of the

³⁰Evidently, μ must be H -invariant.

³¹In the archimedean case with \mathcal{R}_u comparable as convex sets.

³²This can be done by choosing in the Lie algebra $\text{Lie}(\mathbf{G})(\widehat{\mathbb{F}})$ a small enough identity neighborhood fulfilling an analogues condition and taking its image under the exponent.

adelic measure on the homogeneous toral set to $\Gamma \backslash G_S$. For simplicity we use the notation μ_i for both measures. Also, we denote by $\mu_{\mathbf{T}_i}$ the Haar measure on \mathbf{T}_i normalized so that $\mathbf{T}_i(\mathbb{F}) \backslash \mathbf{T}_i(\mathbb{A})$ has volume 1.

$$\begin{aligned}
\mu_i \left(\Gamma x B^{(-\tau_i, \tau_i)} \right) &= \mu_i \left(\mathbf{G}(\mathbb{F}) \delta_0 t_0 g_i k_s B^{(-\tau_i, \tau_i)} \times K_S \right) \\
&= \mu_i \left(\mathbf{G}(\mathbb{F}) t_0 g_i B^{(-\tau_i, \tau_i)} \times K_S \right) \\
&= \mu_{\mathbf{T}_i} \left(t \in \mathbf{T}_i(\mathbb{A}) \mid \exists \delta \in \mathbf{G}(\mathbb{F}) : \delta t g_i \in \delta_0 t_0 g_i B^{(-\tau_i, \tau_i)} \times K_S \right) \\
(28) \quad &= \mu_{\mathbf{T}_i} \left(t \in \mathbf{T}_i(\mathbb{A}) \mid \exists \delta \in \mathbf{G}(\mathbb{F}) : \delta_0^{-1} \delta t \in t_0 \cdot g_i \left(B^{(-\tau_i, \tau_i)} \times K_S \right) g_i^{-1} \right)
\end{aligned}$$

For any $\delta \in \mathbf{G}(\mathbb{F})$ contributing to the measure of the Bowen ball in (28) we have that $\lambda = \delta_0^{-1} \delta$ fulfills the condition of Theorem 8.9, so $\lambda \in \mathbf{T}_i(\mathbb{F})$. In particular, it is enough to take in (28) only $\delta = \delta_0$. This implies

$$\begin{aligned}
\mu_i \left(\Gamma x B^{(-\tau_i, \tau_i)} \right) &= \mu_{\mathbf{T}_i} \left(t \in \mathbf{T}_i(\mathbb{A}) \mid t \in t_0 \cdot g_i \left(B^{(-\tau_i, \tau_i)} \times K_S \right) g_i^{-1} \right) \\
&= \mu_{\mathbf{T}_i} \left(t \in \mathbf{T}_i(\mathbb{A}) \mid t \in g_i \left(B^{(-\tau_i, \tau_i)} \times K_S \right) g_i^{-1} \right) \\
&\leq \mu_{\mathbf{T}_i} \left(t \in \mathbf{T}_i(\mathbb{A}) \mid t \in g_i (B \times K_S) g_i^{-1} \right) \\
(29) \quad &\asymp_B \text{vol}(Y_i)^{-1} = D_i^{-1/2 - o(1)}
\end{aligned}$$

Where the last equality is [ELMV11, Theorem 4.8] (see Remark 8.10).

Combining (27) and (29) and setting $\kappa' = 2\eta(\kappa + 1)$ we see that

$$\begin{aligned}
\mu_i \left(x B^{(-\tau_i, \tau_i)} \right) &\leq \exp \left(- \left(\frac{1}{2} + o(1) \right) \log D_i \right) \\
&= \exp \left(- \left(\frac{1}{2} + o(1) \right) (2\eta\tau_i / (1 + o(1)) - \kappa') \right) \\
&\ll_{\kappa', \varepsilon} \exp(-(\eta - \varepsilon)\tau_i)
\end{aligned}$$

The proof is now concluded. \square

9. RIGIDITY OF LIMIT MEASURES

We now combine Theorem 1.2 with measure rigidity for higher rank torus actions. Specifically, we are going to use the results of [EL15] which generalizes [EKL06].

The following proposition is a simple analogue of [ELMV09, Theorem 5.1] combined with the improved entropy bounds of Theorem 1.2. Its proof is standard and follows the same lines as [ELMV09, Theorem 5.1].

Proposition 9.1. *We assume for simplicity $\mathbb{F} = \mathbb{Q}$. Let $\hat{u} \in S$ and denote $\hat{\mathbb{F}} := \mathbb{F}_{\hat{u}}$. Fix a maximal torus $\mathbf{H} < \mathbf{G}_{\hat{\mathbb{F}}}$ defined over $\hat{\mathbb{F}}$ and set $H := \mathbf{H}(\hat{\mathbb{F}})$. Assume that \mathbf{H} is totally split over $\hat{\mathbb{F}}$.*

Suppose we have a sequence of H invariant homogeneous toral sets of maximal type $Y_i = \mathbf{G}(\mathbb{F}) \backslash \mathbf{T}_i(\mathbb{A}) g_i$ with \mathbf{T}_i a torus defined and anisotropic over \mathbb{F} and $g_i \in G_{\mathbb{A}}$. Let \mathbb{L}_i/\mathbb{F} be the splitting field of \mathbf{T}_i . We assume for all i that $\text{Gal}(\mathbb{L}_i/\mathbb{F})$ is 2-transitive.

Denote by D_i the global discriminant of Y_i and by $D_{\text{ram},i}$ the ramified discriminant of Y_i . Assume $D_i \rightarrow_{i \rightarrow \infty} \infty$ and $D_{\text{ram},i} = D_i^{o(1)}$.

Let μ_i be the probability measure on $\Gamma \backslash G_S$ induced by the probability measure on the homogeneous toral set Y_i . If μ_i converges in the weak-* topology to a probability measure μ on $\Gamma \backslash G_S$ then

$$\mu \geq \int \nu \, d\tau(\nu)$$

Where τ is a finite measure on the space of H invariant Borel probability measures on $\Gamma \backslash G_S$ and

- (1) For τ -almost every ν there is a reductive algebraic subgroup $\mathbf{L} < \mathbf{G}$ defined and anisotropic over \mathbb{Q} and some $g \in G_S$ such that ν is the unique $g^{-1}\mathbf{L}(\mathbb{Q}_S)g$ invariant measure supported on the periodic orbit $\Gamma \backslash \mathbf{L}(\mathbb{Q}_S)g$. Moreover, $H < g_{\hat{u}}^{-1}\mathbf{L}(\hat{\mathbb{F}})g_{\hat{u}}$ and ν is H ergodic.
- (2) For any $a \in H$ we have

$$\int h_{\nu}(a) \, d\tau(\nu) = h_{\mu}(a) \geq \frac{h_{\text{Haar}}(a)}{2(n-1)}$$

$$\text{In particular, } \int d\tau(\nu) \geq \frac{1}{2(n-1)}.$$

Remark 9.2. The reductive subgroups $\mathbf{L} < \mathbf{G}$ appearing in the decomposition above include over $\hat{\mathbb{F}}$ a maximal split torus of $\mathbf{G}_{\hat{\mathbb{F}}}$. In particular, $\mathbf{L}_{\hat{\mathbb{F}}}$ is a reductive subgroup of maximal rank of the split group $\mathbf{G}_{\hat{\mathbb{F}}}$ which has type A_n . By the Borel-de Siebenthal algorithm [BDS49] adapted to algebraic groups, $\mathbf{L}_{\hat{\mathbb{F}}}$ is a semidirect product of a torus – $Z(\mathbf{L}_{\hat{\mathbb{F}}})$ – and groups of type A_k with $k \leq n$.

Proof. Decompose μ into H invariant and ergodic probability measures

$$\mu = \int \nu \, d\tilde{\tau}(\nu)$$

where $\tilde{\tau}$ is a probability measure on the space of H invariant Borel probability measures on $\Gamma \backslash G_S$ supported on the H ergodic measures. Let $\mathcal{P}_{>0}$ be the Borel set³³ of H invariant probability measures ν such that $h_{\nu}(a) > 0$ for some $a \in H$. Define

$$\tau = \tilde{\tau}|_{\mathcal{P}_{>0}}$$

³³ To see that this is a Borel set in the space of probability measures fix a countable dense subset $\{a_i\}_{i=1}^{\infty}$ of the separable space H . It holds that $\mathcal{P}_{>0} = \bigcup_{i=1}^{\infty} \{\nu \mid h_{\nu}(a_i) > 0\}$. Each sets in this union is Borel because we can compute the entropy using a countable set of finite partitions of $\Gamma \backslash G_S$ that generate together the whole σ -algebra.

Obviously, $\mu \geq \int \nu d\tau(\nu)$ and (2) follows from the linearity of the entropy with respect to a fixed $a \in H$ when considered as a function on the convex set of Borel probability measures on $\Gamma \backslash G_S$.

Assertion (1) is a direct consequences of [EL15, Theorem 1.1 and Remark after Corollary 1.2] combined with the fact that, by definition of τ , $h_\nu(a) > 0$ for some $a \in H$ for τ -almost all ν . \square

The following corollary is a modest qualitative restriction on possible limit measures arising from the entropy bound.

Corollary 9.3. *Fix $R \in \mathbb{N}$. Let $\mu \geq \int \nu d\tau(\nu)$ be as in Proposition 9.1. Let $\mathbf{L} < \mathbf{G}$ be a reductive subgroup of maximal rank, such that the rank of all its simple parts (of type A_k) is less than R .*

Set $N_R = (R + 2)(R + 1)R - 1$. If the absolute rank of \mathbf{G} is greater than $N_R - 1$, then $\tau(\{\nu\}) < 1$ for each ν supported on a periodic orbit of a conjugate of $\mathbf{L}(\mathbb{Q}_S)$, namely, μ is not supported on a single periodic orbit of type \mathbf{L} .

Proof. Assume ν is an H invariant and ergodic probability measure on $\Gamma \backslash G$ corresponding to the periodic orbit $\Gamma \backslash \mathbf{L}(\mathbb{Q}_S)g$. Set $\tilde{\mathbf{L}} := g^{-1}\mathbf{L}_{\widehat{\mathbb{F}}}g$ – a reductive split algebraic group over $\widehat{\mathbb{F}}$. Recall that $\mathbf{H} < \tilde{\mathbf{L}}$ is a maximal split torus.

Let $j: \mathbf{SL}_{k_1, \widehat{\mathbb{F}}} \times \dots \times \mathbf{SL}_{k_l, \widehat{\mathbb{F}}} \times \mathbf{T}_0 \rightarrow \tilde{\mathbf{L}}$, where \mathbf{T}_0 is a torus defined over $\widehat{\mathbb{F}}$, be the obvious isogeny from the simply connected cover to $\tilde{\mathbf{L}}$, see Remark 9.2. Let $\mathbf{H}_i < \mathbf{SL}_{k_i, \widehat{\mathbb{F}}}$ a maximal torus whose image under j is contained in \mathbf{H} . By replacing j with a composition of j with an inner automorphism of $\tilde{\mathbf{L}}$ we can assure that $\mathbf{H} = j(\prod_i \mathbf{H}_i \times \mathbf{T}_0)$.

Denote by q the cardinality of the residue field of $\widehat{\mathbb{F}}$ if \widehat{u} is nonarchimedean or $q := \exp(1)$ if \widehat{u} is archimedean. Then by choosing an element $a_i \in \mathbf{H}_i(\widehat{\mathbb{F}})$ and $t_0 \in \mathbf{T}_0(\widehat{\mathbb{F}})$ similarly to Remark 1.3³⁴ For $a := j(a_1, \dots, a_l, t_0) \in H$ we have

$$h_{\text{Haar}}(a) = \log q \frac{(n+1)n(n-1)}{6}$$

$$h_\nu(a) = \log q \sum_{i=1}^l \frac{(k_i+1)k_i(k_i-1)}{6} \leq \log q \frac{n}{2} \frac{(R+2)(R+1)R}{6}$$

and

$$(30) \quad h_\mu(a)/h_{\text{Haar}}(a) \geq \frac{1}{2(n-1)}$$

$$(31) \quad h_\nu(a)/h_{\text{Haar}}(a) \leq \frac{(R+2)(R+1)R}{2(n+1)(n-1)}$$

³⁴Instead of $\exp((n-j)/2)$ one puts $\varpi^{(n-j)/2}$ where ϖ is a uniformizer for $\widehat{\mathbb{F}}$ if \widehat{u} is nonarchimedean and $\varpi = \exp(1)$ otherwise.

Using the inequality

$$\begin{aligned} h_\mu(a) &= \int h_{\nu'}(a) d\tau(\nu') \leq h_\nu(a)\nu(\{\tau\}) + h_{\text{Haar}}(a)(1 - \nu(\{\tau\})) \\ \implies \nu(\{\tau\}) &\leq \frac{h_{\text{Haar}}(a) - h_\mu(a)}{h_{\text{Haar}}(a) - h_\nu(a)} \end{aligned}$$

together with inequalities (30) and (31) we conclude that $\nu(\{\tau\}) < 1$ if $n > (R+2)(R+1)R-1$. \square

REFERENCES

- [AG60] Maurice Auslander and Oscar Goldman. Maximal orders. *Trans. Amer. Math. Soc.*, 97:1–24, 1960.
- [BDS49] A. Borel and J. De Siebenthal. Les sous-groupes fermés de rang maximum des groupes de Lie clos. *Comment. Math. Helv.*, 23:200–221, 1949.
- [Bha04] Manjul Bhargava. Higher composition laws. II. On cubic analogues of Gauss composition. *Ann. of Math. (2)*, 159(2):865–886, 2004.
- [BO07] Yves Benoist and Hee Oh. Equidistribution of rational matrices in their conjugacy classes. *Geom. Funct. Anal.*, 17(1):1–32, 2007.
- [Bor63] Armand Borel. Some finiteness properties of adèle groups over number fields. *Inst. Hautes Études Sci. Publ. Math.*, (16):5–30, 1963.
- [Cas86] J. W. S. Cassels. *Local fields*, volume 3 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 1986.
- [Con12] Brian Conrad. Finiteness theorems for algebraic groups over function fields. *Compos. Math.*, 148(2):555–639, 2012.
- [Dol03] Igor Dolgachev. *Lectures on invariant theory*, volume 296. Cambridge University Press, 2003.
- [Duk88] W. Duke. Hyperbolic distribution problems and half-integral weight Maass forms. *Invent. Math.*, 92(1):73–90, 1988.
- [EKL06] Manfred Einsiedler, Anatole Katok, and Elon Lindenstrauss. Invariant measures and the set of exceptions to Littlewood’s conjecture. *Ann. of Math. (2)*, 164(2):513–560, 2006.
- [EL15] Manfred Einsiedler and Elon Lindenstrauss. On measures invariant under tori on quotients of semisimple groups. *Ann. of Math. (2)*, 181(3):993–1031, 2015.
- [ELMV09] Manfred Einsiedler, Elon Lindenstrauss, Philippe Michel, and Akshay Venkatesh. Distribution of periodic torus orbits on homogeneous spaces. *Duke Math. J.*, 148(1):119–174, 2009.
- [ELMV11] Manfred Einsiedler, Elon Lindenstrauss, Philippe Michel, and Akshay Venkatesh. Distribution of periodic torus orbits and Duke’s theorem for cubic fields. *Ann. of Math. (2)*, 173(2):815–885, 2011.
- [ELMV12] Manfred Einsiedler, Elon Lindenstrauss, Philippe Michel, and Akshay Venkatesh. The distribution of closed geodesics on the modular surface, and Duke’s theorem. *Enseign. Math. (2)*, 58(3-4):249–313, 2012.
- [EMS96] Alex Eskin, Shahar Mozes, and Nimish Shah. Unipotent flows and counting lattice points on homogeneous varieties. *Ann. of Math. (2)*, 143(2):253–299, 1996.
- [EMV13] Jordan S. Ellenberg, Philippe Michel, and Akshay Venkatesh. Linnik’s ergodic method and the distribution of integer points on spheres. In *Automorphic representations and L-functions*, volume 22 of *Tata Inst. Fundam. Res. Stud. Math.*, pages 119–185. Tata Inst. Fund. Res., Mumbai, 2013.

- [GS06] P. Gille and T. Szamuely. *Central Simple Algebras and Galois Cohomology*. Cambridge Studies in Advanced Mathematics. Cambridge University Press, 2006.
- [IS01] P. Ion and J.P. Serre. *Galois Cohomology*. Springer Monographs in Mathematics. Springer Berlin Heidelberg, 2001.
- [Iwa87] Henryk Iwaniec. Fourier coefficients of modular forms of half-integral weight. *Invent. Math.*, 87(2):385–401, 1987.
- [Kem78] George R. Kempf. Instability in invariant theory. *Ann. of Math. (2)*, 108(2):299–316, 1978.
- [Kön16] Dénes König. Über Graphen und ihre Anwendung auf Determinantentheorie und Mengenlehre. *Math. Ann.*, 77(4):453–465, 1916.
- [Lin57] Yu. V. Linnik. Asymptotic-geometric and ergodic properties of sets of lattice points on a sphere. *Mat. Sb. N.S.*, 43(85):257–276, 1957.
- [Lin60] Yu. V. Linnik. Asymptotic-geometric and ergodic properties of sets of lattice points on a sphere. *Amer. Math. Soc. Transl. (2)*, 13:9–27, 1960.
- [Lin68] Yu. V. Linnik. *Ergodic properties of algebraic fields*. Translated from the Russian by M. S. Keane. Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 45. Springer-Verlag New York Inc., New York, 1968.
- [Lin06] Elon Lindenstrauss. Invariant measures and arithmetic quantum unique ergodicity. *Ann. of Math. (2)*, 163(1):165–219, 2006.
- [LM99] David B. Leep and Gerry Myerson. Marriage, magic, and solitaire. *Amer. Math. Monthly*, 106(5):419–429, 1999.
- [MFK94] David Mumford, John Fogarty, and Frances Clare Kirwan. *Geometric invariant theory*, volume 34. Springer Science & Business Media, 1994.
- [MV06] Philippe Michel and Akshay Venkatesh. Equidistribution, L -functions and ergodic theory: on some problems of Yu. Linnik. In *International Congress of Mathematicians. Vol. II*, pages 421–457. Eur. Math. Soc., Zürich, 2006.
- [Nag64] Masayoshi Nagata. Invariants of a group in an affine ring. *J. Math. Kyoto Univ.*, 3:369–377, 1963/1964.
- [Oh04] Hee Oh. Finiteness of compact maximal flats of bounded volume. *Ergodic Theory Dynam. Systems*, 24(1):217–225, 2004.
- [PV94] Vladimir L Popov and Ernest B Vinberg. Invariant theory. In *Algebraic geometry IV*, pages 123–278. Springer, 1994.
- [Rei75] I. Reiner. *Maximal orders*. L.M.S. monographs. Academic Press, 1975.
- [S⁺15] W.A. Stein et al. *Sage Mathematics Software (Version 6.8)*. The Sage Development Team, 2015. <http://www.sagemath.org>.
- [Sku62] B. F. Skubenko. The asymptotic distribution of integers on a hyperboloid of one sheet and ergodic theorems. *Izv. Akad. Nauk SSSR Ser. Mat.*, 26:721–752, 1962.
- [Wal85] J.-L. Waldspurger. Sur les valeurs de certaines fonctions L automorphes en leur centre de symétrie. *Compositio Math.*, 54(2):173–242, 1985.
- [Woo14] Melanie Matchett Wood. Parametrization of ideal classes in rings associated to binary forms. *J. Reine Angew. Math.*, 689:169–199, 2014.

THE EINSTEIN INSTITUTE OF MATHEMATICS, EDMOND J. SAFRA CAMPUS, THE HEBREW UNIVERSITY OF JERUSALEM, GIVAT RAM, JERUSALEM, 9190401, ISRAEL